Θεωρία Galois

Πρόχειρες σημειώσεις

2013-14 (εκδοχή 2-7-2014)

Περιεχόμενα

0. Υπενθυμίσεις και συμπληρώματα

Βασικά σημεία

- Ανάγωγα πολυώνυμα πάνω από το $\mathbb{Q}$.
- Ο δακτύλιος $F[x]/(p(x))$.
- Χαρακτηριστική σώματος.
- Απλές ρίζες πολυωνύμων.

Στην ενότητα αυτή υπενθυμίζουμε και συμπληρώνουμε μερικά αποτελέσματα και έννοιες από τη Βασική Άλγεβρα που θα χρησιμοποιήσουμε πολλές φορές παρακάτω.

Ανάγωγα πολυώνυμα

Έστω F σώμα και $f(x)\in F[x]$ με $\deg f(x)\geq 1$. Υπενθυμίζουμε ότι το $f(x)$ λέγεται **ανάγωγο πάνω από το** F (ή ότι το $f(x)\in F[x]$ είναι ανάγωγο) αν δεν υπάρχουν πολυώνυμα $g(x),h(x)\in F[x]$ με $f(x)=g(x)h(x)$ και $\deg g(x),\deg h(x)\geq 1$. Για παράδειγμα, αν $\deg f(x)=1$, τότε το $f(x)$ είναι ανάγωγο πάνω από το F. Το x^2+1 είναι ανάγωγο πάνω από το $\mathbb{R}$ αλλά δεν είναι ανάγωγο πάνω από το $\mathbb{C}$.

Ξέρουμε ότι αν $\deg f(x)=2,3$, τότε το $f(x)$ είναι ανάγωγο πάνω από το F αν και μόνο αν δεν έχει ρίζα στο F.

Χρειαζόμαστε μερικούς τρόπους να αναγνωρίζουμε ανάγωγα πολυώνυμα πάνω από το $\mathbb{Q}$.

Πρόταση 0.1 *Έστω $f(x)=a_nx^n+\ldots+a_1x+a_0\in\mathbb{Z}[x]$ και $r,s\in\mathbb{Z}$ με $\mu\kappa\delta(r,s)=1$. Αν το r/s είναι ρίζα του $f(x)$, τότε το r διαιρεί το a_0 και το s διαιρεί το r_n.*

Απόδειξη Από $a_n(r/s)^n+\ldots+a_1r/s+a_0=0$ παίρνουμε $a_nr^n+a_nr^{n-1}s+\ldots+a_1rs^{n-1}+a_0s^n=0$. Άρα το r διαιρεί το a_0s^n. Από την υπόθεση $\mu\kappa\delta(r,s)=1$, έπεται ότι το r διαιρεί το a_0. Όμοια το s διαιρεί το a_n.

Παράδειγμα Το $f(x)=x^3+3x+5\in\mathbb{Q}[x]$ είναι ανάγωγο.

Το $f(x)$ δεν έχει ρητή ρίζα γιατί από την προηγούμενη πρόταση οι πιθανές ρητές ρίζες είναι οι $1,-1,5,-5$. Αλλά $f(1)\neq 0, f(-1)\neq 0, f(5)\neq 0, f(-5)\neq 0$. Επειδή $\deg f(x)=3$ και το $f(x)$ δεν έχει ρίζα στο $\mathbb{Q}$, το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Έστω p πρώτος. Έχουμε τον ομομορφισμό δακτυλίων $\mathbb{Z}\to\mathbb{Z}_p, a\mapsto[a]$, όπου $[a]$ είναι η κλάση υπολοίπων του a modulo p. Αν $f(x)=a_nx^n+\ldots+a_0\in\mathbb{Z}[x]$, θέτουμε $\overline{f}(x)=[a_n]x^n+\ldots+[a_0]\in\mathbb{Z}_p[x]$. Εύκολα αποδεικνύεται ότι η απεικόνιση $\mathbb{Z}[x]\to\mathbb{Z}_p[x], f(x)\mapsto\overline{f}(x)$, είναι ομομορφισμός δακτυλίων. Το $\overline{f}(x)$ ονομάζεται η **αναγωγή** του $f(x)$ modulo p. Για παράδειγμα, η αναγωγή modulo 3 του $6x^4-9x+12$ είναι το μηδενικό πολυώνυμο στο $\mathbb{Z}_3[x]$, ενώ η αναγωγή modulo 2 του $6x^4-9x+12$ είναι το πολυώνυμο x του $\mathbb{Z}_2[x]$.

Το ακόλουθο αποτέλεσμα είναι πολύ χρήσιμο όταν θέλουμε να 'συγκρίνουμε' παραγοντοποιήσεις στο $\mathbb{Q}[x]$ και $\mathbb{Z}[x]$. Στην απόδειξη χρησιμοποιούμε αναγωγή modulo p.

Λήμμα 0.2 (Gauss) *Έστω $f(x)\in\mathbb{Z}[x]$ και $g(x),h(x)\in\mathbb{Q}[x]$ με $f(x)=g(x)h(x)$. Τότε υπάρχουν $a(x),b(x)\in\mathbb{Z}[x]$ με $f(x)=a(x)b(x)$, $\deg a(x)=\deg g(x), \deg b(x)=\deg h(x)$.*

Απόδειξη Επειδή $g(x),h(x)\in\mathbb{Q}[x]$, υπάρχουν $c,d\in\mathbb{Z}-\{0\}$ με $cg(x),dh(x)\in\mathbb{Z}[x]$. Άρα στο $\mathbb{Z}[x]$ έχουμε

$$cdf(x)=(cg(x))(dh(x)) \qquad (1)$$

Έστω p πρώτος αριθμός που διαιρεί το cd και $cd = pk$. Τότε η αναγωγή modulo p του $cdf(x)$ είναι το μηδενικό πολυώνυμο, οπότε η αναγωγή modulo p του γινομένου $(cg(x))(dh(x))$ είναι το μηδενικό πολυώνυμο. Επειδή η απεικόνιση $\mathbb{Z}[x] \to \mathbb{Z}_p[x], a(x) \mapsto \overline{a}(x)$, είναι ομομορφισμός δακτυλίων και ο δακτύλιος $\mathbb{Z}_p[x]$ είναι περιοχή, συμπεραίνουμε ότι η αναγωγή modulo p του $cg(x)$ ή του $dh(x)$ είναι το μηδενικό πολυώνυμο, ισοδύναμα ότι κάθε συντελεστής του $cg(x)$ ή του $dh(x)$ είναι πολλαπλάσιο του p. Έστω ότι ισχύει η πρώτη περίπτωση, οπότε έχουμε $cg(x) = pg_1(x), g_1(x) \in \mathbb{Z}[x]$. Τότε από την (1) παίρνουμε

$$kf(x) = g_1(x))(dh(x)) \text{ στο } \mathbb{Z}[x]. \tag{2}$$

Τώρα επαναλαμβάνουμε την ίδια διαδικασία αρχίζοντας με τη (2) στη θέση της (1) για να απλοποιήσουμε έναν πρώτο παράγοντα του k. Συνεχίζοντας έτσι φτάνουμε τελικά σε μια παράσταση της μορφής $\pm f(x) = a(x)b(x)$ όπου $a(x), b(x) \in \mathbb{Z}[x]$ και $\deg a(x) = \deg g(x), \deg b(x) = \deg h(x)$.

Παράδειγμα Το $f(x) = x^4 - 5x^2 + 1 \in \mathbb{Q}[x]$ είναι ανάγωγο.

Από την Πρόταση 0.1 έπεται ότι οι πιθανές ρητές ρίζες του $f(x)$ είναι οι $1, -1$. Αλλά $f(1) \neq 0$ και $f(-1) \neq 0$. Άρα το $f(x)$ δεν έχει ρίζα στο $\mathbb{Q}$.

Συνεπώς αν το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{Q}[x]$, τότε από το Λήμμα 0.2 υπάρχουν $a,b,c,d \in \mathbb{Z}$ με

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 - 5x + 1.$$

Κάνοντας τις πράξεις και εξισώνοντας αντίστοιχους συντελεστές παίρνουμε

$$\begin{cases} a + c = 0 \\ ac + b + d = -5 \\ bc + ad = 0 \\ bd = 1. \end{cases}$$

Άρα $c^2 = b + d + 5$. Αλλά από $bd = 1$ και $b, d \in \mathbb{Z}$ παίρνουμε $b = d = 1$ ή $b = d = -1$. Στην πρώτη περίπτωση παίρνουμε $c^2 = 7$ και στη δεύτερη $c^2 = 3$, που είναι άτοπα. Άρα το $f(x) = x^4 - 5x^2 + 1$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Παρατήρηση Έστω $f(x) \in \mathbb{Z}[x]$ και $g(x), h(x) \in \mathbb{Q}[x]$ με $f(x) = g(x)h(x)$. Από την απόδειξη του Λήμματος 0.2, έπεται ότι υπάρχουν μη μηδενικά $c_1, c_2 \in \mathbb{Q}$ με $a(x) = c_1 g(x)$, $b(x) = c_2 h(x)$ και $f(x) = a(x)b(x)$. Συνεπώς αν υποθέσουμε ότι τα $f(x), g(x), h(x)$ είναι μονικά, συμπεραίνουμε ότι $g(x), h(x) \in \mathbb{Z}[x]$.

Πρόταση 0.3 *Έστω $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ και p πρώτος που δεν διαιρεί το a_n. Αν το $\overline{f}(x)$ είναι ανάγωγο στο $\mathbb{Z}_p[x]$, τότε το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.*

Απόδειξη Αν $f(x) = g(x)h(x)$, όπου $g(x), h(x) \in \mathbb{Q}[x]$ και $\deg f(x), \deg g(x) \geq 1$, από το Λήμμα του Gauss μπορούμε να υποθέσουμε ότι $g(x), h(x) \in \mathbb{Z}[x]$ και $\deg f(x), \deg g(x) \geq 1$. Επειδή το p δεν διαιρεί το a_n, το p δεν διαιρεί ούτε το μεγιστοβάθμιο συντελεστή του $g(x)$ ούτε το μεγιστοβάθμιο συντελεστή του $h(x)$. Άρα $\deg \overline{g}(x) = \deg g(x) \geq 1$ και $\deg \overline{h}(x) = \deg h(x) \geq 1$

Παίρνοντας αναγωγές modulo p προκύπτει $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ και επειδή το $\overline{f}(x)$ είναι ανάγωγο στο $\mathbb{Z}_p[x]$ παίρνουμε ότι το $\overline{g}(x)$ ή το $\overline{g}(x)$ είναι σταθερό πολυώνυμο, άτοπο.

Παράδειγμα Το $f(x) = 15x^4 + 14x^2 + 3x + 35$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Πράγματι, επιλέγοντας $p = 2$, έχουμε $\overline{f}(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. Εύκολα επαληθεύεται ότι το $\overline{f}(x)$ δεν έχει ρίζα στο $\mathbb{Z}_2$. Επίσης, τα μόνο ανάγωγο πολυώνυμο βαθμού 2 στο $\mathbb{Z}_2[x]$ είναι το $x^2 + x + 1$ (γιατί;) και

εύκολα επαληθεύεται με την Ευκλείδεια διαίρεση ότι το x^2+x+1 δεν διαιρεί το $\overline{f}(x)$ στο $\mathbb{Z}_2[x]$. Άρα το $\overline{f}(x)$ είναι ανάγωγο στο $\mathbb{Z}_2[x]$. Από την Πρόταση 0.3, έπεται ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Πρόταση 0.4 (**κριτήριο του Eisenstein**) *Έστω* $f(x)=a_nx^n+\ldots+a_1x+a_0\in\mathbb{Z}[x]$ *πολυώνυμο θετικού βαθμού. Αν υπάρχει πρώτος* p *τέτοιος ώστε*

i) $p|a_0$, $p|a_1,\ldots,p|a_{n-1}$,

ii) p *δεν διαιρεί το* a_n *και*

iii) p^2 *δεν διαιρεί το* a_0,

τότε το $f(x)$ *είναι ανάγωγο στο* $\mathbb{Q}[x]$.

Απόδειξη Έστω $n>1$. Από το Λήμμα 0.2 αρκεί να δείξουμε ότι δεν υπάρχουν $g(x),h(x)\in\mathbb{Z}[x]$ θετικού βαθμού με $f(x)=g(x)h(x)$.

Έστω ότι υπάρχουν τέτοια $g(x),h(x)$. Λαμβάνοντας αναγωγές modulo p έχουμε $\overline{f}(x)=\overline{g}(x)\overline{h}(x)$. Από τις υποθέσεις i) και ii) έπεται ότι $\overline{f}(x)=[a_n]x^n$ και το $[a_n]$ είναι μη μηδενικό. Από τη μοναδικότητα της παραγοντοποίησης πολυωνύμων στο $\mathbb{Z}_p[x]$ σε γινόμενο ανάγωγων παίρνουμε $\overline{g}(x)=bx^m$ και $\overline{h}(x)=cx^l$ για κάποια μη μηδενικά $b,c\in\mathbb{Z}_p$. Έχουμε $m=\deg g(x)>0$ και $l=\deg h(x)>0$. Τότε από $\overline{g}(x)=bx^m$ και $\overline{h}(x)=cx^l$ έπεται ότι το p διαιρεί και το $g(0)$ και το $h(0)$, οπότε το p^2 διαιρεί το $g(0)h(0)=f(0)$, άτοπο.

Παραδείγματα 0.5

i) Αν n είναι θετικός ακέραιος και p πρώτος, τότε το πολυώνυμο x^n-p είναι ανάγωγο στο $\mathbb{Q}[x]$ από το κριτήριο του Eisenstein.

ii) Το $5x^{10}+36x^4+6x^3+12x+12$ είναι ανάγωγο στο $\mathbb{Q}[x]$ από το κριτήριο Eisenstein για $p=3$.

iii) Έστω p πρώτος και $f(x)=x^{p-1}+x^{p-2}+\ldots+x+1\in\mathbb{Q}[x]$. Θα δείξουμε ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ και για το σκοπό αυτό αρκεί να δείξουμε ότι το $f(x+1)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ (γιατί;).

Έχουμε $f(x)=\dfrac{x^p-1}{x-1}$ οπότε

$$f(x+1)=\frac{(x+1)^p-1}{x+1-1}=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\ldots+\binom{p}{p-1}.$$

Ο p διαιρεί καθέναν από τους $\binom{p}{1},\binom{p}{2},\ldots,\binom{p}{p-1}$ (γιατί;), ο p δεν διαιρεί το 1 και ο p^2 δεν διαιρεί το $\binom{p}{p-1}=p$. Από την Πρόταση 0.4 το $f(x+1)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Ανάγωγα πολυώνυμα και σώματα

Αν R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $a\in R$, με (a) συμβολίζουμε το σύνολο $\{ra\in R\,|\,r\in R\}$. Το (a) είναι ιδεώδες του R. Ειδικά, αν $R=F[x]$, όπου F σώμα, και $p(x)\in F[x]$ έχουμε το ιδεώδες $I=(p(x))=\{f(x)p(x)\,|\,f(x)\in F[x]\}$. Ξέρουμε ότι ο δακτύλιος πηλίκο $F[x]/I$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο (το 1_F+I) ως προς τις πράξεις

$$F[x]/I\times F[x]/I\to F[x]/I,\quad (a(x)+I,b(x)+I)\mapsto a(x)+b(x)+I,$$
$$F[x]/I\times F[x]/I\to F[x]/I,\quad (a(x)+I,b(x)+I)\mapsto a(x)b(x)+I$$

Υπενθυμίζουμε το παρακάτω αποτέλεσμα.

Πρόταση 0.6 *Έστω F σώμα, $p(x) \in F[x]$ και $I = (p(x))$. Το $p(x)$ είναι ανάγωγο αν και μόνο αν ο δακτύλιος πηλίκο $F[x]/I$ είναι σώμα.*

Απόδειξη Έστω ότι το $p(x)$ είναι ανάγωγο. Ξέρουμε ότι ο δακτύλιος $F[x]/I$ είναι μεταθετικός και έχει μοναδιαίο στοιχείο το $1_F + I$. Επειδή $\deg p(x) \geq 1$, έχουμε $I \neq F[x]$, οπότε ο δακτύλιος $F[x]/I$ είναι μη μηδενικός.

Έστω $f(x) + I \in F[x]/I$, $f(x) + I \neq 0_{F[x]/I} = I$. Τότε $f(x) \notin I$, δηλαδή το $p(x)$ δεν διαιρεί το $f(x)$. Επειδή το $p(x)$ είναι ανάγωγο έχουμε $\mu\kappa\delta(f(x), p(x)) = 1$ και επομένως υπάρχουν $a(x), b(x) \in F[x]$ με

$$1_F = a(x)f(x) + b(x)p(x).$$

Τότε στο $F[x]/I$ έχουμε $1_F + I = (a(x) + I)(f(x) + I)$, δηλαδή το $f(x) + I$ είναι αντιστρέψιμο στοιχείο. Άρα ο δακτύλιος $F[x]/I$ είναι σώμα.

Αντίστροφα, έστω ότι ο δακτύλιος $F[x]/I$ είναι σώμα και έστω $p(x) = a(x)b(x)$, όπου $a(x), b(x) \in F[x]$, $\deg a(x) < \deg p(x)$ και $\deg b(x) < \deg p(x)$. Τότε στο $F[x]/I$ ισχύει $0_{F[x]/I} = I = (a(x) + I)(b(x) + I)$. Επειδή ο $F[x]/I$ είναι σώμα παίρνουμε $a(x) + I = 0_{F[x]/I}$ ή $b(x) + I = 0_{F[x]/I}$, δηλαδή $a(x) \in I$ ή $b(x) \in I$, ισοδύναμα $p(x) \mid a(x)$ ή $p(x) \mid b(x)$. Αυτό σημαίνει ότι $\deg a(x) \geq \deg p(x)$ ή $\deg b(x) \geq \deg p(x)$, άτοπο.

Παραδείγματα

i) Είδαμε πριν ότι το $p(x) = x^4 - 5x^2 + 1 \in \mathbb{Q}[x]$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Άρα ο δακτύλιος $\mathbb{Q}[x]/(p(x))$ είναι σώμα.

ii) Επειδή το $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ δεν έχει ρίζα στο $\mathbb{Z}_2$ και έχει βαθμό 3, είναι ανάγωγο στο $\mathbb{Z}_2[x]$. Άρα ο δακτύλιος πηλίκο $\mathbb{Z}_2[x]/(p(x))$ είναι σώμα.

Χαρακτηριστική σώματος

Έστω F σώμα. Εύκολα αποδεικνύεται ότι η απεικόνιση $f : \mathbb{Z} \to F, m \mapsto m1_F$, είναι ομομορφισμός δακτυλίων. Ο πυρήνας $\ker f$ είναι ιδεώδες του $\mathbb{Z}$ και άρα έχει τη μορφή $(p) = \{ap \in \mathbb{Z} \mid a \in \mathbb{Z}\}$ για μοναδικό μη αρνητικό ακέραιο p. Ο p λέγεται η **χαρακτηριστική** του σώματος F. Από το πρώτο θεώρημα ισομορφισμών δακτυλίων έχουμε ότι ο δακτύλιος $\mathbb{Z}/(p)$ είναι ισόμορφος με υποδακτύλιο του σώματος F. Άρα ο $\mathbb{Z}/(p)$ δεν έχει μηδενοδιαιρέτες. Επιπλέον ο $\mathbb{Z}/(p)$ είναι μη μηδενικός αφού $f(1) = 1_F \neq 0_F$. Συνεπώς ο μη αρνητικός ακέραιος p είναι ή 0 ή πρώτος αριθμός. Στην πρώτη περίπτωση, εύκολα επαληθεύεται ότι η απεικόνιση $\mathbb{Q} \to F, m/n \mapsto m1_F(n1_F)^{-1}$, είναι μονομορφισμός. Στη δεύτερη περίπτωση έχουμε μονομορφισμό $\mathbb{Z}_p \to F$.

Για παράδειγμα, για κάθε πρώτο p η χαρακτηριστική του $\mathbb{Z}_p$ είναι p. Η χαρακτηριστική καθενός των $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι 0.

Συνοψίζοντας, έχουμε το την εξής πρόταση.

Πρόταση 0.7 *Έστω F σώμα. Ισχύουν τα εξής.*

i) Αν η χαρακτηριστική του F είναι 0, τότε υπάρχει μονομορφισμός σωμάτων $\mathbb{Q} \to F$.

ii) Έστω πρώτος p. Αν η χαρακτηριστική του F είναι p, τότε υπάρχει μονομορφισμός σωμάτων $\mathbb{Z}_p \to F$. Στην περίπτωση αυτή, ο p είναι ο μικρότερος θετικός ακέραιος m τέτοιος ώστε $ma = 0_F$ για κάθε $a \in F$.

Απλές ρίζες πολυωνύμων

Έστω $f(x) \in K[x]$, όπου K σώμα, και $a \in K$ ρίζα του $f(x)$. Τότε το $x-a$ διαιρεί το $f(x)$ στο $K[x]$. Αν το $(x-a)^2$ δεν διαιρεί το $f(x)$ στο $K[x]$, θα λέμε ότι το a είναι **απλή ρίζα** του $f(x)$ στο K. Μια ρίζα που δεν είναι απλή λέγεται **πολλαπλή**. Για παράδειγμα, το 1 είναι απλή ρίζα του $(x-1)(x+5)^2 \in \mathbb{Q}[x]$ και το -5 είναι πολλαπλή ρίζα του $(x-1)(x+5)^2 \in \mathbb{Q}[x]$.

Αν F είναι σώμα και $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, ορίζουμε την τυπική παράγωγο $f'(x)$ του $f(x)$ ως $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1 \in F[x]$. Εύκολα επαληθεύονται οι γνώριμες σχέσεις

$$(cf(x)) = cf'(x),$$
$$(f(x)+g(x))' = f'(x)+g'(x),$$
$$(f(x)g(x))' = f'(x)g(x)+f(x)g'(x),$$

για κάθε $c \in F$ και $f(x), g(x) \in F[x]$.

Παράδειγμα Για $f(x) = x^p + x + 1 \in \mathbb{Z}_p[x]$, όπου p πρώτος, έχουμε $f'(x) = px^{p-1} + 1 + 0 = 1$, γιατί στο $\mathbb{Z}_p[x]$, $pg(x) = 0$ για κάθε $g(x) \in \mathbb{Z}_p[x]$.

Το ακόλουθο αποτέλεσμα είναι συχνά χρήσιμο όταν θέλουμε να αποφανθούμε ότι μια ρίζα είναι απλή. Για την απόδειξή του υπενθυμίζουμε ότι αν F είναι υπόσωμα σώματος K και $f(x), g(x) \in F[x]$, τότε ο μέγιστος κοινός διαιρέτης των $f(x), g(x)$ όταν αυτά θεωρηθούν ως στοιχεία του $F[x]$ ταυτίζεται με το μέγιστο κοινό διαιρέτη των $f(x), g(x)$ όταν αυτά θεωρηθούν ως στοιχεία του $K[x]$ (γιατί;).

Πρόταση 0.8 *Έστω F υπόσωμα σώματος K, $f(x) \in F[x]$ και $a \in K$ ρίζα του $f(x)$.*

i) Αν $\mu\kappa\delta(f(x), f'(x)) = 1$, τότε το a είναι απλή ρίζα του $f(x)$.

ii) Αν η χαρακτηριστική του F είναι 0 και το $f(x)$ είναι ανάγωγο πάνω από το F, τότε το a είναι απλή ρίζα του $f(x)$. Ειδικά κάθε ανάγωγο $f(x) \in \mathbb{Q}[x]$ έχει μόνο απλές ρίζες στο $\mathbb{C}$.

Απόδειξη Έστω ότι το a είναι πολλαπλή ρίζα του $f(x)$, δηλαδή $f(x) = (x-a)^2 g(x)$ για κάποιο $g(x) \in K[x]$. Τότε $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$. Άρα το $x-a$ διαιρεί το $f'(x)$ στο $K[x]$, οπότε το $x-a$ διαιρεί το $\mu\kappa\delta(f(x), f'(x))$ στο $K[x]$. Συνεπώς έχουμε $\mu\kappa\delta(f(x), f'(x)) \neq 1$

i) Άμεσο από αυτό που είπαμε πριν.

ii) Αν το $f(x)$ είναι ανάγωγο πάνω από το F, τότε από $\mu\kappa\delta(f(x), f'(x)) \neq 1$, παίρνουμε $\mu\kappa\delta(f(x), f'(x)) = c^{-1}f(x)$, όπου c ο μεγιστοβάθμιος όρος του $f(x)$. Άρα το $f(x)$ διαιρεί το $f'(x)$. Επειδή $\deg f'(x) < \deg f(x)$, παίρνουμε $f'(x) = 0$. Αυτό είναι αδύνατο γιατί $\deg f(x) \geq 1$ και η χαρακτηριστική του F είναι 0.

Παράδειγμα 0.9 Έστω n θετικός ακέραιος, F υπόσωμα σώματος K και $f(x) = x^n - 1 \in F[x]$. Αν η χαρακτηριστική του F είναι 0 ή πρώτος p που δεν διαιρεί το n, τότε κάθε ρίζα του $f(x)$ στο K είναι απλή.

Πράγματι, έχουμε $f'(x) = nx^{n-1}$ και λόγω της υπόθεσης στη χαρακτηριστική του F, το nx^{n-1} δεν είναι το μηδενικό πολυώνυμο. Είναι σαφές ότι $\mu\kappa\delta(f(x), f'(x)) = \mu\kappa\delta(x^n - 1, nx^{n-1}) = 1$ και το ζητούμενο έπεται από την Πρόταση 0.8 i).

Το πολυώνυμο $x^4 - 1 \in \mathbb{Z}_2[x]$ έχει πολλαπλή ρίζα στο $\mathbb{Z}_2$ αφού $x^4 - 1 = (x-1)^4$ στο $\mathbb{Z}_2[x]$.

Ασκήσεις 0

1. Ποια από τα ακόλουθα πολυώνυμα είναι ανάγωγα πάνω από το $\mathbb{Q}$;

a. $x^3 + x + 6$.
b. $x^4 + 2x^3 + x + 1$.
c. $9x^4 + 4x^3 - 3x + 125$.
d. $2x^5 - x^3 + 4x - 5$.
e. $x^5 + \frac{1}{3}x^4 + \frac{3}{5}x^3 + \frac{5}{7}x + \frac{7}{9}$.
f. $x^5 - 6x^4 - 12x + 12$.

2. Υπάρχουν άπειροι το πλήθος ακέραιοι a για τους οποίους το πολυώνυμο $x^7 + 15x^2 - 30x + a$ είναι ανάγωγο πάνω από το $\mathbb{Q}$.
3. Δείξτε ότι τα ακόλουθα πολυώνυμα είναι ανάγωγα.
   a. $x^8 + 1 \in \mathbb{Q}[x]$.
   b. $1 + x + \frac{x^2}{2!} + \ldots + \frac{x^p}{p!} \in \mathbb{Q}[x]$, όπου p πρώτος.
4. Δείξτε τα αντίστροφα στην Πρόταση 0.7.
5. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.
   a. Οι ρίζες του $x^5 + x + 1$ στο $\mathbb{C}$ είναι απλές.
   b. Ο δακτύλιος $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$ είναι σώμα.
   c. Για κάθε $n \in \mathbb{Z}_{>0}$ υπάρχουν άπειρα το πλήθος ανάγωγα πολυώνυμα στο $\mathbb{Q}[x]$ βαθμού n.
   d. Αν F είναι υπόσωμα σώματος K, τότε τα F και K έχουν την ίδια χαρακτηριστική.
   e. Αν F σώμα και $f(x) \in F[x]$ ανάγωγο, τότε τα σώματα F και $F[x]/(f(x))$ έχουν την ίδια χαρακτηριστική.
   f. Έστω $f(x) \in \mathbb{Q}[x]$ μονικό πολυώνυμο τέτοιο ώστε $f(x) \mid x^{100} - 1$ στο $\mathbb{Q}[x]$. Τότε $f(x) \in \mathbb{Z}[x]$.

1. Επεκτάσεις σωμάτων

Βασικά σημεία

- Ελάχιστο πολυώνυμο.
- Βαθμός διαδοχικών επεκτάσεων.
- Παραδείγματα υπολογισμού βαθμών επεκτάσεων.
- Θεώρημα επέκτασης ισομορφισμών.

Ορισμοί

Αν K είναι σώμα και F υπόσωμα του K, θα λέμε ότι το K είναι **επέκταση** του F. Για παράδειγμα, το $\mathbb{C}$ είναι επέκταση του $\mathbb{R}$, το $\mathbb{R}$ είναι επέκταση του $\mathbb{Q}$ και το $\mathbb{C}$ είναι επέκταση του $\mathbb{Q}$.

Αν το K είναι επέκταση του F, τότε το K είναι F - διανυσματικός χώρος με εξωτερικό πολλαπλασιασμό $F\times K\to K,(a,b)\mapsto ab,$ και θα συμβολίζουμε τη διάσταση $\dim_F K$ με $[K:F]$. Ο ακέραιος $[K:F]$ λέγεται ο **βαθμός** της επέκτασης $F\subseteq K$. Για παράδειγμα, $[\mathbb{C}:\mathbb{R}]=2$ γιατί μια βάση του $\mathbb{C}$ ως $\mathbb{R}$ - διανυσματικός χώρος είναι το σύνολο $\{1,i\}$.

Μια επέκταση K του F λέγεται **πεπερασμένη** αν $[K:F]<\infty$ και **άπειρη** αν δεν είναι πεπερασμένη. Για παράδειγμα, η επέκταση $\mathbb{C}$ του $\mathbb{R}$ είναι πεπερασμένη.

Έστω K επέκταση του F και $S\subseteq K$.

- Με $F(S)$ συμβολίζουμε την τομή όλων των υποσωμάτων του K που περιέχουν το F και το S. Το $F(S)$ είναι σώμα και $F\subseteq F(S)\subseteq K$.
- Αν το σύνολο S είναι πεπερασμένο $S=\{a_1,...,a_n\}$ συμβολίζουμε το σώμα $F(S)$ με $F(a_1,..,a_n)$.

Πρόταση 1.1 *Έστω K επέκταση του F και $a_1,...,a_n\in K$. Έχουμε*

i) $F(a_1,...,a_n)=\left\{\dfrac{f(a_1,...,a_n)}{g(a_1,...,a_n)}\in K\,\middle|\, f(x_1,...,x_n),g(x_1,...,x_n)\in F[x_1,...,x_n],\ g(a_1,...,a_n)\neq 0\right\}$.

ii) $F(a_1,...,a_n)=F_1(a_n)$, *όπου* $F_1=F(a_1,...,a_{n-1})$.

Απόδειξη i) Εύκολα αποδεικνύεται ότι το δεξί μέλος, έστω E, είναι σώμα τέτοιο ώστε $F\subseteq E\subseteq K$ και $a_1,...,a_n\in E$. Από τον ορισμό του $F(a_1,...,a_n)$ έπεται ότι $F(a_1,...,a_n)\subseteq E$.

Αν L είναι σώμα με $F\subseteq L$ και $a_1,...,a_n\in L$, τότε $\dfrac{f(a_1,...,a_n)}{g(a_1,...,a_n)}\in L$ για κάθε $f(x_1,...,x_n),g(x_1,...,x_n)\in F[x_1,...,x_n],\ g(a_1,...,a_n)\neq 0$ από τον ορισμό του σώματος. Άρα $L\supseteq E$. Από τον ορισμό του $F(a_1,...,a_n)$ έπεται ότι $F(a_1,...,a_n)\supseteq E$. Συνεπώς $F(a_1,...,a_n)=E$.

ii) Άμεσο από τον ορισμό.

Παράδειγμα Ισχύει $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Πράγματι, επειδή $\sqrt{2}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ και $\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ έχουμε $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. Επειδή το $\mathbb{Q}(\sqrt{2},\sqrt{3})$ είναι σώμα τέτοιο ώστε $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$ και $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, έχουμε

$$\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3}).$$

Έστω $a=\sqrt{2}+\sqrt{3}$. Έχουμε $a\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ και άρα $a^{-1}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Αλλά

$$a^{-1}=\frac{1}{\sqrt{2}+\sqrt{3}}=\frac{\sqrt{2}-\sqrt{3}}{(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3})}=-\sqrt{2}+\sqrt{3}.$$

Αφού $\sqrt{2}=\frac{1}{2}(a-a^{-1})$ και $\sqrt{3}=\frac{1}{2}(a+a^{-1})$, παίρνουμε $\sqrt{2}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ και $\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Επειδή το σώμα $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ περιέχει το $\mathbb{Q}$ και τα $\sqrt{2},\sqrt{3}$, έχουμε

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Άρα $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Αλγεβρικά στοιχεία, ελάχιστο πολυώνυμο

Ορισμός 1.2 *Έστω K επέκταση του F και $a \in K$. Θα λέμε ότι το a είναι **αλγεβρικό πάνω από το** F αν υπάρχει μη μηδενικό πολυώνυμο $f(x) \in F[x]$ με $f(a) = 0$.*

Παραδείγματα

i) Για παράδειγμα, το $\sqrt{2}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$ αφού είναι ρίζα του $x^2 - 2 \in \mathbb{Q}[x]$.

ii) Το $a = \sqrt[3]{1+\sqrt{2}}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$. Πράγματι, έχουμε $a^3 = 1+\sqrt{2}$ οπότε $(a^3-1)^2 = 2$ δηλαδή $a^6 - 2a^3 - 1 = 0$. Άρα το a είναι ρίζα του $x^6 - 2x^3 - 1 \in \mathbb{Q}[x]$.

iii) Το $\sqrt{2}+\sqrt{3}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$ αφού είναι ρίζα του $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ (γιατί;).

iv) Αποδεικνύεται ότι το π δεν είναι αλγεβρικό πάνω από το $\mathbb{Q}$ (βλ. Θεώρημα 4.4.1 στο βιβλίο του Ανδρεαδάκη).

v) Το π είναι αλγεβρικό πάνω από το $\mathbb{Q}(\pi)$ αφού είναι ρίζα του $x - \pi \in \mathbb{Q}(\pi)[x]$.

Έστω K επέκταση του F και $a \in K$ αλγεβρικό πάνω από το F. Τότε υπάρχει μη μηδενικό $f(x) \in F[x]$ με $f(a) = 0$. Πολλαπλασιάζοντας με τον αντίστροφο του μεγιστοβάθμιου συντελεστή, μπορούμε να υποθέσουμε ότι το $f(x)$ είναι μονικό. Συνεπώς το σύνολο των μονικών πολυωνύμων του $F[x]$ που έχουν ρίζα το a είναι μη κενό. Θεωρούμε ένα πολυώνυμο $p(x)$ του συνόλου αυτού που έχει ελάχιστο βαθμό. Το $p(x)$ είναι μοναδικό. Πράγματι, αν $q(x) \in F[x]$ είναι μονικό, έχει ρίζα το a και είναι ελαχίστου βαθμού, τότε $\deg p(x) = \deg q(x)$ και συνεπώς $\deg(p(x) - q(x)) < \deg p(x)$. Έχουμε $p(a) - q(a) = 0$ και συνεπώς αν $p(x) - q(x) \neq 0$, τότε πολλαπλασιάζοντας με τον αντίστροφο του μεγιστοβάθμιου συντελεστή του $p(x) - q(x)$ θα είχαμε μονικό πολυώνυμο που έχει ρίζα το a και έχει βαθμό μικρότερο από το βαθμό του $p(x)$. Άρα $p(x) - q(x) = 0$.

Θα καλούμε αυτό το $p(x)$ το **ελάχιστο πολυώνυμο του a πάνω από το F** και θα το συμβολίζουμε με $Irr(a,F)$.

Για παράδειγμα, $Irr(\sqrt{2},\mathbb{R}) = x - \sqrt{2}$. Επίσης, $\deg Irr(\sqrt{2},\mathbb{Q}) > 1$ γιατί αλλιώς $\sqrt{2} \in \mathbb{Q}$ που δεν ισχύει. Συνεπώς $Irr(\sqrt{2},\mathbb{Q}) = x^2 - 2$.

Ακολουθούν μερικές ιδιότητες του $Irr(a,F)$.

Πρόταση 1.3 *Έστω K επέκταση του F και $a \in K$ αλγεβρικό πάνω από το F. Τότε*

i) Το $Irr(a,F) \in F[x]$ είναι ανάγωγο.

ii) Αν $f(x) \in F[x]$ έχει ρίζα το a, τότε $Irr(a,F) \mid f(x)$.

iii) Αν $q(x) \in F[x]$ είναι μονικό ανάγωγο πολυώνυμο με ρίζα το a, τότε $q(x) = Irr(a,F)$.

Απόδειξη i) Εξ ορισμού $\deg Irr(a,F) \geq 1$. Αν το $Irr(a,F)$ δεν ήταν ανάγωγο πάνω στο F, τότε το a θα ήταν ρίζα κάποιου μονικού γνήσιου παράγοντα του $Irr(a,F)$, πράγμα αδύνατο λόγω του ελαχίστου του βαθμού του $Irr(a,F)$.

ii) Έστω $f(x) \in F[x]$ με $f(a) = 0$. Από την Ευκλείδεια διαίρεση, υπάρχουν $q(x), r(x) \in F[x]$ με $f(x) = q(x)Irr(a,F) + r(x)$ και $\deg r(x) < \deg Irr(a,F)$. Άρα $r(a) = f(a) = 0$. Αν το $r(x)$ είναι μη μηδενικό, τότε πολλαπλασιάζοντας με τον αντίστροφο του μεγιστοβάθμιου συντελεστή του $r(x)$ θα είχαμε ένα μονικό πολυώνυμο στο $F[x]$ με ρίζα το a και βαθμό μικρότερο του βαθμού του $Irr(a,F)$, άτοπο.

iii) Από το ii) έπεται ότι $Irr(a,F) \mid q(x)$. Επειδή το $q(x)$ είναι ανάγωγο και το $Irr(a,F)$ θετικού βαθμού παίρνουμε $q(x) = cIrr(a,F)$ για κάποιο $c \in F$. Επειδή τα $q(x), Irr(a,\mathbb{Q})$ είναι μονικά έχουμε $c = 1$.

Παραδείγματα 1.4

i) Έστω n θετικός ακέραιος και p πρώτος. Στο Παράδειγμα 0.5 είδαμε ότι το $x^n - p$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Από την Πρόταση 1.3 iii) έχουμε $Irr(\sqrt[n]{p}, \mathbb{Q}) = x^n - p$.

ii) Έστω p πρώτος και $\zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} \in \mathbb{C}$. Επειδή $\zeta_p{}^p = 1$, $\zeta_p \neq 1$ και $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + ... + x + 1)$, το ζ_p είναι ρίζα του $x^{p-1} + x^{p-2} + ... + x + 1$. Στο Παράδειγμα 0.5 είδαμε ότι το πολυώνυμο αυτό είναι ανάγωγο πάνω από το $\mathbb{Q}$ και επομένως από την Πρόταση 1.3 iii) έχουμε $Irr(\zeta_p, \mathbb{Q}) = x^{p-1} + x^{p-2} + ... + x + 1$.

Στην επόμενη πρόταση περιγράφονται σημαντικές διασυνδέσεις μεταξύ του πολυωνύμου $Irr(a, F)$ και του σώματος $F(a)$.

Πρόταση 1.5 *Έστω K επέκταση του F, $a \in K$ αλγεβρικό πάνω από το F, $p(x) = Irr(a, F)$ και $n = \deg p(x)$. Τότε*

i) Τα σώματα $F(a)$ και $F[x]/(p(x))$ είναι ισόμορφα.

ii) Μια βάση του F - διανυσματικού χώρου $F(a)$ είναι το σύνολο $\{1, a, a^2, ..., a^{n-1}\}$. Άρα $[F(a) : F] = n$.

iii) Αν $f(x) \in F[x]$ είναι μη μηδενικό τέτοιο ώστε $f(a) = 0$, τότε $[F(a) : F] \leq \deg f(x)$.

Απόδειξη i) Επειδή το $p(x) \in F[x]$ είναι ανάγωγο, ο δακτύλιος $F[x]/(p(x))$ είναι σώμα σύμφωνα με την Πρόταση 0.6. Θεωρούμε την απεικόνιση $\varphi_a : F[x] \to F(a), f(x) \mapsto f(a)$. Εύκολα επαληθεύεται ότι αυτή είναι ομομορφισμός δακτυλίων και $(p(x)) \subseteq \ker\varphi_a$. Από την Πρόταση 1.3 ii) έπεται ότι $(p(x)) \supseteq \ker\varphi_a$ και επομένως $(p(x)) = \ker\varphi_a$. Συνεπώς από το πρώτο θεώρημα ισομορφισμών δακτυλίων, οι δακτύλιοι $F[x]/(p(x))$ και $\mathrm{Im}\,\varphi_a$ είναι ισόμορφοι. Άρα ο δακτύλιος $\mathrm{Im}\,\varphi_a$ είναι σώμα. Θα δείξουμε στη συνέχεια ότι $\mathrm{Im}\,\varphi_a = F(a)$.

Έχουμε $\mathrm{Im}\,\varphi_a = \{f(a) \,|\, f(x) \in F[x]\}$ και επομένως από την Πρόταση 1.1 έπεται ότι $\mathrm{Im}\,\varphi_a \subseteq F(a)$. Από την άλλη μεριά, είναι σαφές ότι $F \subseteq \mathrm{Im}\,\varphi_a$ και $a \in \mathrm{Im}\,\varphi_a$. Επειδή ο δακτύλιος $\mathrm{Im}\,\varphi_a$ είναι σώμα παίρνουμε $F(a) \subseteq \mathrm{Im}\,\varphi_a$. Άρα $\mathrm{Im}\,\varphi_a = F(a)$.

ii) Αν $c_0 + c_1 a + ... + c_{n-1}a^{n-1} = 0$, όπου $c_i \in F$, τότε το πολυώνυμο $c_0 + c_1 x + ... + c_{n-1}x^{n-1} \in F[x]$ έχει ρίζα το a ενώ ο βαθμός του είναι μικρότερος του $n = \deg Irr(a, F)$. Άρα είναι το μηδενικό πολυώνυμο, δηλαδή $c_0 = c_1 = ... = c_{n-1} = 0$. Άρα τα στοιχεία $1, a, ..., a^{n-1}$ είναι γραμμικά ανεξάρτητα πάνω από το F.

Στην απόδειξη του i) είδαμε ότι $F(a) = \mathrm{Im}\,\varphi_a = \{f(a) \,|\, f(x) \in F[x]\}$. Δηλαδή κάθε στοιχείο του $F(a)$ είναι της μορφής $f(a)$, όπου $f(x) \in F[x]$. Από την Ευκλείδεια διαίρεση, υπάρχουν $q(x), r(x) \in F[x]$ με $f(x) = q(x)p(x) + r(x)$ και $\deg r(x) < n$. Άρα $f(a) = r(a)$. Επειδή $r(x) = r_0 + r_1 x + ... + r_{n-1}x^{n-1}$, όπου $r_i \in F$, τα στοιχεία $1, a, ..., a^{n-1}$ παράγουν το F - διανυσματικό χώρο $F(a)$.

iii) Αν $f(x) \in F[x]$ είναι μη μηδενικό τέτοιο ώστε $f(a) = 0$, τότε από τον ορισμό του $Irr(a, F)$ έχουμε $\deg f(x) \geq \deg p(x)$. Το ζητούμενο έπεται από σχέση $[F(a) : F] = \deg p(x)$ του ii).

Παραδείγματα 1.6

i) Επειδή $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, μια βάση του $\mathbb{Q}$ - διανυσματικού χώρου $\mathbb{Q}(\sqrt{2})$ είναι το σύνολο $\{1, \sqrt{2}\}$. Έχουμε $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Κάθε στοιχείο του $\mathbb{Q}(\sqrt{2})$ γράφεται μοναδικά στη μορφή $a + b\sqrt{2}$, όπου $a, b \in \mathbb{Q}$.

ii) Επειδή $Irr(\sqrt[3]{2},\mathbb{Q})=x^3-2$ (Παράδειγμα 1.4 i)), μια βάση του $\mathbb{Q}$ - διανυσματικού χώρου $\mathbb{Q}(\sqrt[3]{2})$ είναι το σύνολο $\{1,\sqrt[3]{2},(\sqrt[3]{2})^2\}=\{1,\sqrt[3]{2},\sqrt[3]{4}\}$. Έχουμε $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. Κάθε στοιχείο του $\mathbb{Q}(\sqrt[3]{2})$ γράφεται μοναδικά στη μορφή $a_1+a_2\sqrt[3]{2}+a_3\sqrt[3]{4}$ όπου $a_i\in\mathbb{Q}$.

iii) Έστω p πρώτος και $\zeta_p=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}\in\mathbb{C}$. Στο Παράδειγμα 1.4 ii) είδαμε ότι $Irr(\zeta_p,\mathbb{Q})=x^{p-1}+x^{p-2}+...+x+1$. Άρα μια βάση του $\mathbb{Q}$ - διανυσματικού χώρου $\mathbb{Q}(\zeta_p)$ είναι η $\{1,\zeta_p,\zeta_p{}^2,...,\zeta_p{}^{p-2}\}$ και $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$.

iv) Θεωρούμε το πολυώνυμο $f(x)=x^3+x^2-x+1$ και $a\in\mathbb{C}$ μια ρίζα του. Το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ γιατί είναι τρίτου βαθμού και δεν έχει ρίζα στο $\mathbb{Q}$ (βλ. Πρόταση 0.1). Επειδή είναι μονικό, έχουμε $Irr(a,\mathbb{Q})=f(x)$ σύμφωνα με την Πρόταση 1.3 iii). Από την Πρόταση 1.5 ii), μια βάση του $\mathbb{Q}$ - διανυσματικού χώρου $\mathbb{Q}(a)$ είναι το σύνολο $\{1,a,a^2\}$.

a. Έστω $b=a^4-2a^2+3a+1\in\mathbb{Q}(a)$. Ας παραστήσουμε το b ως γραμμικό συνδυασμό των $1,a,a^2$. Με την Ευκλείδεια διαίρεση βρίσκουμε ότι $x^4-2x^2+3x+1=(x-1)f(x)+x+2$. Άρα $b=2+a$.

b. Έστω $c=(a-1)^{-1}\in\mathbb{Q}(a)$. Ας παραστήσουμε το c ως γραμμικό συνδυασμό των $1,a,a^2$.
$1^{ος}$ τρόπος. Επειδή το a είναι ρίζα του $f(x)$, το $a-1$ είναι ρίζα του
$$f(x+1)=(x+1)^3+(x+1)^2-(x+1)+1=x^3+4x^2+4x+2=x(x^2+4x+4)+2.$$
Από $(a-1)((a-1)^2+4(a-1)+4)+2=0$, παίρνουμε
$$(a-1)^{-1}=-\frac{1}{2}((a-1)^2+4(a-1)+4)=-\frac{1}{2}(a^2+2a+1).$$
$2^{ος}$ τρόπος. Με τη βοήθεια του Ευκλείδειου αλγορίθμου (όπως θυμόμαστε από τη Βασική Άλγεβρα) υπολογίζουμε $a(x),b(x)\in\mathbb{Q}[x]$ τέτοια ώστε μκδ$(f(x),x-1)=$ $a(x)f(x)+b(x)(x-1)$. Βρίσκουμε $1=\frac{1}{2}f(x)+(-\frac{1}{2}x^2-x-\frac{1}{2})(x-1)$. Άρα στο $\mathbb{Q}(a)$ έχουμε $1=(-\frac{1}{2}a^2+a-\frac{1}{2})(a-1)$. Συνεπώς $(a-1)^{-1}=-\frac{1}{2}a^2-a-\frac{1}{2}$.

Παρατηρήσεις

i) Στην απόδειξη της Πρότασης 1.5 είδαμε ότι αν το a είναι αλγεβρικό πάνω από το F, τότε
$$F(a)=\{f(a)\,|\,f(x)\in F[x]\}.$$
Σημειώνουμε ότι το συμπέρασμα αυτό δεν αληθεύει αν το a δεν είναι αλγεβρικό πάνω από το F. Πράγματι, αν ο δακτύλιος $\{f(a)\,|\,f(x)\in F[x]\}$ είναι σώμα, τότε $a^{-1}\in\{f(a)\,|\,f(x)\in F[x]\}$, οπότε $a^{-1}=f(a)$ για κάποιο $f(x)\in F[x]$. Άρα το a είναι ρίζα του πολυωνύμου $xf(x)-1$ που είναι μη μηδενικό και έχει συντελεστές στο F. Δηλαδή το a είναι αλγεβρικό πάνω από το F. (Βλ. σχετικά την άσκηση 1.14).

ii) Έστω $F\subseteq F(a_1,...,a_n)$ επέκταση όπου κάθε a_i είναι αλγεβρικό πάνω από το F. Τότε
$$F(a_1,...,a_n)=\{f(a_1,...,a_n)\,|\,f(x_1,...,x_n)\in F[x_1,...,x_n]\}.$$
Έχουμε δείξει την περίπτωση $n=1$ και η γενική περίπτωση προκύπτει εύκολα με επαγωγή (άσκηση). Καλό είναι να συγκριθεί το αποτέλεσμα αυτό με την Πρόταση 1.1 i).

Βαθμοί διαδοχικών επεκτάσεων

Θεώρημα 1.7 *Έστω διαδοχικές επεκτάσεις* $F\subseteq K\subseteq L$. *Αν* $[K:F]<\infty$ *και* $[L:K]<\infty$, *τότε* $[L:F]<\infty$ *και*
$$[L:F]=[L:K][K:F].$$

Σχηματικά έχουμε το εξής διάγραμμα.

$$\begin{matrix} & L & \\ [L:F] & \left\{ \begin{matrix} | \\ \} [L:K] \\ K \\ | \\ \} [K:F] \end{matrix} \right. & \\ & F & \end{matrix}$$

Απόδειξη Έστω $\{a_1,...,a_n\}$ μια βάση του K ως F διανυσματικός χώρος και έστω $\{b_1,...,b_m\}$ μια βάση του L ως K διανυσματικός χώρος. Θα δείξουμε ότι τα στοιχεία

$$a_i b_j,\ i=1,...,n,\ j=1,...,m$$

αποτελούν βάση του L ως F διανυσματικός χώρος.

Έστω $c \in L$. Τότε υπάρχουν $r_i \in K$ με

$$c = r_1 b_1 + r_2 b_2 + ... + r_m b_m .$$

Για κάθε i υπάρχουν $s_{i1},..,s_{in} \in F$ με $r_i = s_{i1}a_1 + ... + s_{in}a_n$. Αντικαθιστώντας έχουμε

$$c = (s_{11}a_1 + ... + s_{1n}a_n)b_1 + (s_{21}a_1 + ... + s_{2n}a_n)b_2 + ... + (s_{m1}a_1 + ... + s_{mn}a_n)b_m =$$
$$= s_{11}a_1b_1 + ... + s_{1n}a_nb_1 + s_{21}a_1b_2 + ... + s_{2n}a_nb_2 + ... + s_{m1}a_1b_m + ... + s_{mn}a_nb_m.$$

Άρα τα στοιχεία $a_i b_j$ παράγουν το διανυσματικό χώρο L πάνω από το F.

Έστω $r_{ij} \in F$ με $\sum_{i=1,j=1}^{n,m} r_{ij}a_ib_j = 0$. Τότε

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} r_{ij}a_i\right)b_j = 0 .$$

Από τη γραμμική ανεξαρτησία των b_j πάνω από το K παίρνουμε

$$\sum_{i=1}^{n} r_{ij}a_i = 0$$

για κάθε $j=1,...,m$. Τότε από τη γραμμική ανεξαρτησία των a_i πάνω από το F παίρνουμε $r_{ij}=0$ για κάθε $j=1,...,m$ και $i=1,...,n$. Άρα τα στοιχεία a_ib_j είναι γραμμικά ανεξάρτητα πάνω από το F.

Παρατήρηση Επαγωγικά προκύπτει το εξής. Έστω διαδοχικές πεπερασμένες επεκτάσεις

$$F_0 \subseteq F_1 \subseteq ... \subseteq F_{n-1} \subseteq F_n .$$

Τότε $[F_n : F_0] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}]...[F_1 : F_0]$.

Παραδείγματα 1.8

i) Θα δείξουμε ότι $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$.

Θεωρούμε τις διαδοχικές επεκτάσεις

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$$

οπότε από το Θεώρημα 1.7 έχουμε

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] .$$

Είδαμε πριν ότι $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Θα δείξουμε παρακάτω ότι $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, οπότε θα έχουμε $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Επειδή το $\sqrt{3}$ μηδενίζει το $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$, έχουμε $\deg Irr(\sqrt{3}, \mathbb{Q}(\sqrt{2})) \le 2$ οπότε $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \le 2$ σύμφωνα με την Πρόταση 1.5 iii). Θα δείξουμε ότι $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$ και για το σκοπό αυτό αρκεί να δείξουμε ότι $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Αν $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ τότε $\sqrt{3} = a + b\sqrt{2}$ για κάποια $a,b \in \mathbb{Q}$, οπότε $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Επειδή το σύνολο $\{1, \sqrt{2}\}$

είναι γραμμικά ανεξάρτητο πάνω από το $\mathbb{Q}$ (Παράδειγμα 1.6 i)), παίρνουμε $2ab=0$, δηλαδή $a=0$ ή $b=0$. Στην πρώτη περίπτωση έχουμε $\sqrt{3}=b\sqrt{2}$ και στη δεύτερη $\sqrt{3}=a$, που είναι άτοπα καθώς $a,b\in\mathbb{Q}$. Άρα $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]>1$ και επειδή είχαμε $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\le 2$ παίρνουμε $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$.

$$\begin{array}{c}\mathbb{Q}(\sqrt{2},\sqrt{3})\\ 4\left\{\begin{array}{c}|\\ \mathbb{Q}(\sqrt{2})\\ |\end{array}\right.\begin{array}{l}\}\,2\\ \\ \}\,2\end{array}\\ \mathbb{Q}\end{array}$$

Παρατήρηση Η απόδειξη του Θεωρήματος 1.7 δίνει ένα τρόπο να βρούμε βάση του $\mathbb{Q}(\sqrt{2},\sqrt{3})$ πάνω από το $\mathbb{Q}$. Επειδή $Irr(\sqrt{2},\mathbb{Q})=x^2-2$,

μια βάση του $\mathbb{Q}(\sqrt{2})$ πάνω από το $\mathbb{Q}$ είναι το σύνολο $\{1,\sqrt{2}\}$,

σύμφωνα με την Πρόταση 1.4. Επειδή $Irr(\sqrt{3},\mathbb{Q}(\sqrt{2}))=x^2-3$,

μια βάση του $\mathbb{Q}(\sqrt{2},\sqrt{3})$ πάνω από το $\mathbb{Q}(\sqrt{2})$ είναι το $\{1,\sqrt{2}\}$.

Από την απόδειξη του Θεωρήματος 1.6, έπεται ότι

μια βάση του $\mathbb{Q}(\sqrt{2},\sqrt{3})$ πάνω από το $\mathbb{Q}$ είναι το $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.

Σημειώνουμε ότι μπορούμε να εφαρμόσουμε την Πρόταση 1.5 απευθείας στο $\mathbb{Q}(\sqrt{2},\sqrt{3})$: Είδαμε σε προηγούμενο παράδειγμα ότι $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Επειδή $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4,$ από την Πρόταση 1.5 έπεται ότι

μια βάση του $\mathbb{Q}(\sqrt{2},\sqrt{3})$ πάνω από το $\mathbb{Q}$ είναι το $\{1,a,a^2,a^3\}$, όπου $a=\sqrt{2}+\sqrt{3}$.

ii) Έστω $\rho=\sqrt[3]{5}$ και $\omega=(-1+i\sqrt{3})/2$. Ισχύει $[\mathbb{Q}(\rho,\omega):\mathbb{Q}]=6$.

Πράγματι, έχουμε τις επεκτάσεις

$$\mathbb{Q}\subseteq\mathbb{Q}(\rho)\subseteq\mathbb{Q}(\rho,\omega).$$

Από $Irr(\sqrt[3]{5},\mathbb{Q})=x^3-5$ (Παράδειγμα 1.4 i)) έπεται ότι (Πρόταση 1.5)

$$[\mathbb{Q}(\rho):\mathbb{Q}]=\deg Irr(\rho,\mathbb{Q})=3.$$

Επειδή $\omega\notin\mathbb{R}$ και $\mathbb{Q}(\rho)\subseteq\mathbb{R}$, έχουμε $\omega\notin\mathbb{Q}(\rho)$ και άρα $\mathbb{Q}(\rho,\omega)\neq\mathbb{Q}(\rho)$. Δηλαδή $[\mathbb{Q}(\rho,\omega):\mathbb{Q}(\rho)]>1$. Επειδή το ω είναι ρίζα του $x^2+x+1\in\mathbb{Q}(\rho)[x]$, έχουμε (Πρόταση 1.5) $[\mathbb{Q}(\rho,\omega):\mathbb{Q}(\rho)]=\deg Irr(\omega,\mathbb{Q}(\rho))\le 2$. Άρα

$$[\mathbb{Q}(\rho,\omega):\mathbb{Q}(\rho)]=2.$$

Από το Θεώρημα 1.7

$$[\mathbb{Q}(\rho,\omega):\mathbb{Q}]=[\mathbb{Q}(\rho,\omega):\mathbb{Q}(\rho)][\mathbb{Q}(\rho):\mathbb{Q}]=2\cdot 3=6.$$

$$\begin{array}{c}\mathbb{Q}(\rho,\omega)\\ 6\left\{\begin{array}{c}|\\ \mathbb{Q}(\rho)\\ |\end{array}\right.\begin{array}{l}\}\,2\\ \\ \}\,3\end{array}\\ \mathbb{Q}\end{array}$$

Παρατήρηση Όπως στην παρατήρηση στο προηγούμενο παράδειγμα έχουμε ότι

μια βάση του $\mathbb{Q}(\rho)$ πάνω από το $\mathbb{Q}$ είναι το σύνολο $\{1,\rho,\rho^2\}$ και

μια βάση του $\mathbb{Q}(\rho,\omega)$ πάνω από το $\mathbb{Q}(\rho)$ είναι το $\{1,\omega\}$.

Από την απόδειξη του Θεωρήματος 1.7, έπεται ότι

μια βάση του $\mathbb{Q}(\rho,\omega)$ πάνω από το $\mathbb{Q}$ είναι το $\{1,\rho,\rho^2,\omega,\rho\omega,\rho^2\omega\}$.

Επεκτείνοντας ισομορφισμούς

Έστω $\tau : F_1 \to F_2$ ισομορφισμός σωμάτων. Εύκολα αποδεικνύεται ότι η απεικόνιση

$$F_1[x] \to F_2[x],\ c_n x^n + c_{n-1}x^{n-1} + ... + c_0 \mapsto \tau(c_n)x^n + \tau(c_{n-1})x^{n-1} + ... + \tau(c_0)$$

είναι ισομορφισμός δακτυλίων. Καταχρηστικά θα τον συμβολίζουμε πάλι με τ. Για παράδειγμα, αν $\tau : \mathbb{C} \to \mathbb{C}$, $\tau(z) = \overline{z}$, όπου $\overline{z}$ είναι ο συζυγής μιγαδικός του z, τότε $\tau((2+3i)x + 4 - i) = (2-3i)x + 4 + i$. Παρατηρούμε ότι αν $f(x) \in F_1[x]$, τότε τα πολυώνυμα $f(x)$ και $\tau(f(x))$ έχουν τον ίδιο βαθμό. Από αυτό έπεται ότι το $f(x) \in F_1[x]$ είναι ανάγωγο αν και μόνο αν το $\tau(f(x)) \in F_2[x]$ είναι ανάγωγο. Στα παρακάτω θα εφαρμόσουμε πολλές φορές το εξής αποτέλεσμα.

Θεώρημα 1.9 (επέκτασης ισομορφισμών) *Έστω $\tau : F_1 \to F_2$ ισομορφισμός σωμάτων, $p(x) \in F_1[x]$ ανάγωγο, a μια ρίζα του $p(x)$ σε κάποια επέκταση του F_1 και b μια ρίζα του $\tau(p(x))$ σε κάποια επέκταση του F_2. Τότε υπάρχει ισομορφισμός σωμάτων $\sigma : F_1(a) \to F_2(b)$ τέτοιος ώστε $\sigma(a) = b$ και $\sigma(c) = \tau(c)$ για κάθε $c \in F_1$.*

$$\begin{array}{ccc} F_1(a) & \xrightarrow{\ \sigma\ } & F_2(b) \\ | & & | \\ F_1 & \xrightarrow{\ \tau\ } & F_2 \end{array}$$

Απόδειξη Έστω Ψ η παρακάτω σύνθεση ομομορφισμών δακτυλίων

$$F_1[x] \xrightarrow{\ \tau\ } F_2[x] \xrightarrow{\ \pi\ } F_2[x]/(\tau(p(x)))$$

όπου $\pi(f(x)) = f(x) + (\tau(p(x)))$. Η Ψ είναι επί γιατί είναι σύνθεση επί απεικονίσεων. Επίσης εύκολα επαληθεύεται ότι $Ker\Psi = (p(x))$. Συνεπώς υπάρχει ισομορφισμός δακτυλίων

$$\tilde{\Psi} : F_1[x]/(p(x)) \to F_2[x]/(\tau(p(x))),$$
$$f(x) + (p(x)) \mapsto \tau(f(x)) + (\tau(p(x))).$$

Έστω σ η παρακάτω σύνθεση

$$F_1(a) \xrightarrow{\ \tilde{\varphi}_a^{-1}\ } F_1[x]/(p(x)) \xrightarrow{\ \tilde{\Psi}\ } F_2[x]/(\tau(p(x)) \xrightarrow{\ \tilde{\varphi}_b\ } F_2(b),$$

όπου

$$\tilde{\varphi}_a : F_1[x]/(p(x)) \to F_1(a)$$

είναι ο ισομορφισμός που επάγεται από τον επιμορφισμό $\varphi_a : F_1[x] \to F_1(a),\ f(x) \to f(a)$ και ομοίως για $\tilde{\varphi}_b$. Τότε η σ είναι ισομορφισμός ως σύνθεση ισομορφισμών. Επίσης $\sigma(a) = b$ και $\sigma(c) = \tau(c)$ για κάθε $c \in F_1$. Πράγματι,

$$a \xrightarrow{\ \tilde{\varphi}_a^{-1}\ } a + (p(x)) \xrightarrow{\ \tilde{\Psi}\ } a + (\tau(p(x))) \xrightarrow{\ \tilde{\varphi}_b\ } b$$

και

$$c \xrightarrow{\ \tilde{\varphi}_a^{-1}\ } c + (p(x)) \xrightarrow{\ \tilde{\Psi}\ } \tau(c) + (\tau(p(x))) \xrightarrow{\ \tilde{\varphi}_b\ } \tau(c).$$

Ο περιορισμός της απεικόνισης $\sigma : F_1(a) \to F_2(b)$ του συμπεράσματος του Θεωρήματος 1.9 στο υποσύνολο $F_1 \subseteq F_1(a)$ είναι η απεικόνιση $\tau : F_1 \to F_2$ της υπόθεσης. Θα λέμε ότι η σ **επεκτείνει** την τ.

Πόρισμα 1.10 *Έστω K επέκταση του F και $a, b \in K$ αλγεβρικά πάνω από το F. Τότε $Irr(a,F) = Irr(b,F)$ αν και μόνο αν υπάρχει ισομορφισμός $\sigma : F(a) \to F(b)$ τέτοιος ώστε $\sigma(a) = b$ και $\sigma(c) = c$ για κάθε $c \in F$.*

Απόδειξη Αν $Irr(a,F) = Irr(b,F)$, το συμπέρασμα έπεται άμεσα από το Θεώρημα 1.9 για $F_1 = F_2 = F$ και $\tau : F \to F$ την ταυτοτική απεικόνιση $\tau = 1_F$.

Αντίστροφα, έστω ότι υπάρχει ισομορφισμός $\sigma : F(a) \to F(b)$ τέτοιος ώστε $\sigma(a) = b$ και $\sigma(c) = c$ για κάθε $c \in F$. Τότε το $\sigma(p(x))$ είναι ανάγωγο, όπου $p(x) = Irr(a, F)$. Αλλά $\sigma(p(x)) = p(x)$ καθώς $\sigma(c) = c$ για κάθε $c \in F$. Επίσης

$$p(b) = p(\sigma(a)) = \sigma(p(a)) = \sigma(0) = 0.$$

Άρα $p(x) = Irr(b, F)$ σύμφωνα με την Πρόταση 1.3 iii).

Στοιχεία a, b όπως στο Πόρισμα 1.10, δηλαδή ρίζες του ίδιου ανάγωγου πολυωνύμου με συντελεστές από το F, λέγονται **συζυγή πάνω από το** F. Για παράδειγμα,

τα συζυγή του $\sqrt{2}+\sqrt{3}$ πάνω από το $\mathbb{Q}$ είναι τα $\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}+\sqrt{3}, -\sqrt{2}-\sqrt{3}$, ενώ

τα συζυγή του $\sqrt{2}+\sqrt{3}$ πάνω από το $\mathbb{Q}(\sqrt{2})$ είναι τα $\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}$.

Αφήνουμε ως άσκηση την επαλήθευση των παραπάνω.

Το Θεώρημα 1.9 χρησιμοποιείται συχνά για την κατασκευή ισομορφισμών 'ειδικών' σωμάτων όπως δείχνει το επόμενο παράδειγμα.

Παράδειγμα 1.11 Έστω $\rho = \sqrt[3]{5}$, $\omega = (-1 + i\sqrt{3})/2$ και $K = \mathbb{Q}(\rho, \omega)$. Θα δείξουμε ότι υπάρχει ισομορφισμός $\sigma : K \to K$ με

$$\sigma(\rho) = \rho\omega^2,$$
$$\sigma(\omega) = \omega^2,$$
$$\sigma(c) = c \text{ για κάθε } c \in \mathbb{Q}.$$

1ο βήμα. Τα στοιχεία $\rho, \rho\omega^2$ είναι ρίζες του πολυωνύμου $x^3 - 5$ που είναι ανάγωγο πάνω από το $\mathbb{Q}$ (Παράδειγμα 1.4 i)). Άρα $Irr(\rho, \mathbb{Q}) = Irr(\rho\omega^2, \mathbb{Q}) = x^3 - 5$. Από το Πόρισμα 1.10 υπάρχει ισομορφισμός $\sigma_1 : \mathbb{Q}(\rho) \to \mathbb{Q}(\rho\omega^2)$ τέτοιος ώστε $\sigma_1(\rho) = \rho\omega^2$ και $\sigma_1(c) = c$ για κάθε $c \in \mathbb{Q}$.

$$\begin{array}{ccc} \mathbb{Q}(\rho) & \xrightarrow{\sigma_1} & \mathbb{Q}(\rho\omega^2) \\ | & & | \\ \mathbb{Q} & \xrightarrow{\tau = 1_{\mathbb{Q}}} & \mathbb{Q} \end{array}$$

2ο βήμα. Θεωρούμε τον ισομορφισμό $\sigma_1 : \mathbb{Q}(\rho) \to \mathbb{Q}(\rho\omega^2)$ που κατασκευάσαμε στο προηγούμενο βήμα και τις επεκτάσεις $\mathbb{Q}(\rho) \subseteq \mathbb{Q}(\rho, \omega) = K$ και $\mathbb{Q}(\rho\omega^2) \subseteq \mathbb{Q}(\rho\omega^2, \omega^2)$ Ισχύει $\mathbb{Q}(\rho\omega^2, \omega^2) = \mathbb{Q}(\rho, \omega)$ αφού $\rho\omega^2, \omega^2 \in \mathbb{Q}(\rho, \omega)$ και $\rho, \omega \in \mathbb{Q}(\rho\omega^2, \omega^2)$ καθώς $\omega = \omega^4$. Το στοιχείο ω είναι ρίζα του πολυωνύμου $x^2 + x + 1$ που είναι ανάγωγο στο $\mathbb{Q}(\rho)[x]$ (γιατί;). Επίσης το ω^2 είναι ρίζα του $\sigma_1(x^2 + x + 1) = x^2 + x + 1$. Από το Θεώρημα 1.9 υπάρχει ισομορφισμός $\sigma_2 : K \to K$ τέτοιος ώστε $\sigma_2(\omega) = \omega^2$ και $\sigma_2(c) = \sigma_1(c)$ για κάθε $c \in \mathbb{Q}(\rho)$.

$$\begin{array}{ccc} K & \xrightarrow{\sigma_2} & K \\ | & & | \\ \mathbb{Q}(\rho) & \xrightarrow{\sigma_1} & \mathbb{Q}(\rho\omega^2) \end{array}$$

Ο ισομορφισμός σ_2 ικανοποιεί τις ζητούμενες ιδιότητες καθώς $\sigma_2(\rho) = \sigma_1(\rho) = \rho\omega^2$, $\sigma_2(\omega) = \omega^2$ και $\sigma_2(c) = \sigma_1(c) = 1_{\mathbb{Q}}(c) = c$ για κάθε $c \in \mathbb{Q}$.

Σημείωση. Σχηματικά θα λέγαμε ότι στην απόδειξη του παραδείγματος 'συμπληρώσαμε' το παρακάτω διάγραμμα εργαζόμενοι από κάτω προς τα πάνω.

$$\begin{array}{ccc} K & \xrightarrow{\sigma_2} & K \\ | & & | \\ \mathbb{Q}(\rho) & \xrightarrow{\sigma_1} & \mathbb{Q}(\rho\omega^2) \\ | & & | \\ \mathbb{Q} & \xrightarrow{\tau=1_{\mathbb{Q}}} & \mathbb{Q} \end{array}$$

Ύπαρξη ρίζας σε επέκταση

Έστω F σώμα και $p(x)\in F[x]$ ανάγωγο πολυώνυμο. Ξέρουμε ότι ο δακτύλιος πηλίκο $F[x]/(p(x))$ είναι σώμα. Εύκολα επαληθεύεται ότι η απεικόνιση $F\to F[x]/(p(x)),\ a\mapsto a+(p(x)),$ είναι μονομορφισμός σωμάτων. Μέσω αυτής θα ταυτίζουμε κάθε $a\in F$ με την εικόνα του στο $F[x]/(p(x))$. Κατά τον τρόπο αυτό θεωρούμε το σώμα $F[x]/(p(x))$ ως επέκταση του F.

Θεώρημα 1.12 *Έστω F σώμα και $f(x)\in F[x]$ με $\deg f(x)\ge 1$. Τότε υπάρχει επέκταση του F όπου το $f(x)$ έχει ρίζα.*

Απόδειξη Επειδή $\deg f(x)\ge 1$ υπάρχει ανάγωγο $p(x)\in F[x]$ που διαιρεί το $f(x)$. Έστω $I=(p(x))$, το κύριο ιδεώδες του $F[x]$ που παράγεται από το $p(x)$. Η απεικόνιση $\psi: F\to F[x]/I,\ a\mapsto a+I,$ είναι μονομορφισμός σωμάτων. Μέσω αυτού θα ταυτίζουμε κάθε $a\in F$ με την εικόνα $a+I$ στο $F[x]/I$. Συνεπώς έχουμε μια επέκταση $F[x]/I$ του F.

Έστω $E=F[x]/I$ και $\alpha=x+I\in E$. Τότε το α είναι ρίζα του $f(x)$ στο E. Πράγματι, αν $f(x)=a_nx^n+\ldots+a_1x+a_0$, τότε υπολογίζοντας στο E έχουμε

$$\begin{aligned} f(\alpha) &= a_n\alpha^n+\ldots+a_1\alpha+a_0 = \\ &= a_n(x+I)^n+\ldots+a_1(x+I)+a_0 = \\ &= a_n(x^n+I)+\ldots+a_1(x+I)+a_0 = \\ &= a_nx^n+\ldots+a_1x+a_0+I = f(x)+I = I = 0_E \end{aligned}$$

αφού $f(x)\in I$ καθώς το $p(x)$ διαιρεί το $f(x)$.

Παραδείγματα

i) Με το συμβολισμό του θεωρήματος, έστω $F=\mathbb{R}$ και $f(x)=x^2+1$. Το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{R}$ και ο δακτύλιος $E=\mathbb{R}[x]/(f(x))$ είναι σώμα. Το $f(x)$ δεν έχει ρίζα στο $\mathbb{R}$, αλλά έχει ρίζα στο E καθώς αν $\alpha=x+(f(x))$, τότε

$$\alpha^2+1+(f(x))=(x+(f(x)))^2+1+f(x)=x^2+1+(f(x))=0_E.$$

Σημειώνουμε ότι το σώμα E είναι ισόμορφο με το σώμα $\mathbb{C}$ των μιγαδικών αριθμών.

ii) Θεωρούμε το $f(x)=x^5+2x^2+2x+2\in\mathbb{Z}_3[x]$. Η ανάλυση του $f(x)$ σε γινόμενο ανάγωγων στο $\mathbb{Z}_3[x]$ είναι $f(x)=(x^2+1)(x^3+2x+2)$ (άσκηση). Οι δακτύλιοι $\mathbb{Z}_3[x]/(x^2+1)$ και $\mathbb{Z}_3[x]/(x^3+2x+2)$ είναι σώματα (Πρόταση 0.6) και σε καθένα από αυτά το $f(x)$ έχει ρίζα σύμφωνα με την απόδειξη του Θεωρήματος 1.12.

Ασκήσεις 1

1. Δείξτε τα εξής.
   a. $\mathbb{Q}(\sqrt{2},\sqrt{5})=\mathbb{Q}(\sqrt{2}+\sqrt{5})$.
   b. $\sqrt{2}\notin\mathbb{Q}(\sqrt{5})$.

c. $[\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}]=4$.

d. $Irr(\sqrt{2}+\sqrt{5},\mathbb{Q})=x^4-14x^2+9$.

e. Το σύνολο $\{1,\sqrt{2},\sqrt{5},\sqrt{10}\}$ είναι μια βάση του $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{Q}(\sqrt{2},\sqrt{5})$.

2. Έστω επέκταση $F\subseteq K$ με $[K:F]$ πρώτο αριθμό. Να βρεθούν όλα τα σώματα L με $F\subseteq L\subseteq K$.

3. Βρείτε τα ακόλουθα ελάχιστα πολυώνυμα

a. $Irr(\sqrt{1+\sqrt{7}},\mathbb{Q})$.

b. $Irr(\sqrt{1+\sqrt{7}},\mathbb{Q}(\sqrt{7}))$.

c. $Irr(\sqrt{2}+i,\mathbb{R})$.

d. $Irr(\sqrt{2}+i,\mathbb{Q})$.

4. Έστω $\zeta_5=\cos(2\pi/5)+i\sin(2\pi/5)\in\mathbb{C}$ και $a=\zeta_5+\zeta_5^{-1}$. Δείξτε τα εξής.

a. $Irr(a,\mathbb{Q})=x^2+x-1$.

b. $\mathbb{Q}(a)=\mathbb{Q}(\sqrt{5})$ και $\cos(2\pi/5)=(-1+\sqrt{5})/4$.

5. Έστω p πρώτος και $a=\sqrt{p+\sqrt{p}}\in\mathbb{R}$. Βρείτε το $Irr(a,\mathbb{Q})$ και το $Irr(a,\mathbb{Q}(\sqrt{p}))$.

6.

a. Έστω K σώμα με $K\subseteq\mathbb{C}$ και $[K:\mathbb{Q}]=9$. Αληθεύει ότι το K περιέχει ρίζα του x^5+3x^2+6x+3;

b. Έστω $a_1,...,a_n\in\mathbb{C}$ με $a_i^2\in\mathbb{Q}$ για κάθε i. Δείξτε ότι $[\mathbb{Q}(a_1,...,a_n):\mathbb{Q}]=2^t$ για κάποιο $t\geq 0$. Αληθεύει ότι $\sqrt[3]{2}\in\mathbb{Q}(a_1,...,a_n)$;

7. Έστω επέκταση $F\subseteq K$ και $a\in K$ αλγεβρικό στοιχείο πάνω από το F τέτοιο ώστε $\deg Irr(a,F)$ είναι περιττός. Τότε $F(a)=F(a^2)$.

8.

a. Έστω $F\subseteq K$ επέκταση και $a,b\in K$ αλγεβρικά στοιχεία πάνω από το F με $[F(a):F]=m,[F(b):F]=n$, όπου $\mu\kappa\delta(m,n)=1$. Τότε $\left[F(a,b):F\right]=mn$.

b. Ποιος είναι ο βαθμός $[\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2}):\mathbb{Q}]$;

9. Έστω $F\subseteq E\subseteq K$ διαδοχικές επεκτάσεις, $a\in K$ και $[K:F]<\infty$. Τότε

a. $[E(a):E]\leq[F(a):F]$ και

b. $[E(a):F(a)]\leq[E:F]$.

10. Έστω $p(x),q(x)\in\mathbb{Q}[x]$ ανάγωγα πολυώνυμα, $a\in\mathbb{C}$ ρίζα του $p(x)$, $b\in\mathbb{C}$ ρίζα του $q(x)$, $F=\mathbb{Q}(a)$ και $K=\mathbb{Q}(b)$. Τότε το $p(x)$ είναι ανάγωγο στο $K[x]$ αν και μόνο αν το $q(x)$ είναι ανάγωγο στο $F[x]$.

11. Έστω $a\in\mathbb{C}$ ρίζα του x^3-x^2+x+1 και $b=\dfrac{a^2}{a-2}$. Να βρεθούν $c_0,c_1,c_2\in\mathbb{Q}$ με $b=c_0+c_1a+c_2a^2$.

12. Στις επόμενες περιπτώσεις εξετάστε αν υπάρχει ισομορφισμός σωμάτων $\sigma:K\to K$ με τις αναγραφόμενες ιδιότητες.

a. $K=\mathbb{Q}(\sqrt{2},i),\sigma(\sqrt{2})=i$.

b. $K=\mathbb{Q}(\sqrt{2},i),\sigma(\sqrt{2})=-\sqrt{2}$.

c. $K=\mathbb{Q}(\rho,\omega),\sigma(\rho)=\rho\omega,\sigma(\omega)=\omega^2$, όπου $\rho=\sqrt[3]{5}$, $\omega=(-1+i\sqrt{3})/2$.

13. Έστω $F\subseteq K$ πεπερασμένη επέκταση και $p(x)\in F[x]$ ανάγωγο. Δείξτε ότι αν $\mu\kappa\delta(\deg p(x),[K:F])=1$, τότε το $p(x)$ είναι ανάγωγο στο $K[x]$.

14. Έστω K επέκταση του σώματος F και $a\in F$. Με $F[a]$ συμβολίζουμε το δακτύλιο $\{f(a)\in K\,|\,f(x)\in F[x]\}$. Δείξτε ότι οι ακόλουθες προτάσεις είναι ισοδύναμες.

a. Το a είναι αλγεβρικό πάνω από το F.

b. $F[a] = F(a)$.

c. Ο δακτύλιος $F[a]$ είναι σώμα.

15. Έστω $F \subseteq K$ επέκταση και $a \in K$ αλγεβρικό πάνω από το F. Θεωρούμε την απεικόνιση $T : F(a) \to F(a), T(b) = ab.$

a. Δείξτε ότι η T είναι γραμμική απεικόνιση (ως απεικόνιση F - διανυσματικών χώρων).

b. Ξέρουμε ότι το σύνολο $\{1, a, ..., a^{n-1}\}$ είναι βάση του $F(a)$ πάνω από το F, όπου $n = \deg Irr(a, F)$. Δείξτε ότι αν $Irr(a, F) = x^n + a_{n-1}x^{n-1} + ... + a_0$, τότε ο πίνακας της T ως προς την προηγούμενη βάση είναι ο

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

c. Δείξτε ότι το ελάχιστο πολυώνυμο του παραπάνω πίνακα (με την έννοια της Γραμμικής Άλγεβρας) ισούται με το $Irr(a, F)$.

16. Εξετάστε ποιες από τις επόμενες προτάσεις είναι αληθείς.

a. $\dfrac{7}{2 + 3\sqrt{10}} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

b. Έστω $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n) \in \mathbb{C}$. Τότε $\zeta_5 \in \mathbb{Q}(\zeta_7)$.

c. Τα σώματα $\mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(i\sqrt[4]{2})$ είναι ισόμορφα.

d. Τα στοιχεία $1, \sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}$ είναι γραμμικά ανεξάρτητα πάνω από το $\mathbb{Q}$.

e. Αν $[\mathbb{Q}(a) : \mathbb{Q}] = 5$, τότε $[\mathbb{Q}(a^3) : \mathbb{Q}] = 5$.

f. $\mathbb{Q}(\rho, \omega) = \mathbb{Q}(\rho\omega)$, όπου $\rho = \sqrt[3]{5}$, $\omega = (-1 + i\sqrt{3})/2$.

g. $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{6})] = 2$.

2. Αλγεβρικές επεκτάσεις, γεωμετρικές κατασκευές

Βασικά σημεία

- Αλγεβρικές επεκτάσεις.
- Κατασκευάσιμα σημεία έχουν συντεταγμένες που είναι αλγεβρικά πάνω από το $\mathbb{Q}$ με βαθμούς δυνάμεις του 2.
- Τα κλασικά προβλήματα κατασκευών με κανόνα και διαβήτη.

Αλγεβρικές επεκτάσεις

Ορισμός 2.1 *Μια επέκταση $F \subseteq K$ λέγεται **αλγεβρική** αν κάθε στοιχείο του K είναι αλγεβρικό πάνω από το F.*

Παραδείγματα

i) Η επέκταση $\mathbb{R} \subseteq \mathbb{C}$ είναι αλγεβρική γιατί κάθε $z \in \mathbb{C}$ είναι ρίζα του $x^2 - (z+\overline{z})x + z\overline{z}$ που έχει πραγματικούς συντελεστές.

ii) Η επέκταση $\mathbb{Q} \subseteq \mathbb{C}$ δεν είναι αλγεβρική γιατί υπάρχουν μιγαδικοί αριθμοί που δεν είναι αλγεβρικοί πάνω από το $\mathbb{Q}$ (Cantor).
Μία σκιαγράφηση μιας απόδειξης είναι: Για κάθε θετικό ακέραιο n έστω $\mathbb{Q}_n[x] = \{f(x) \in \mathbb{Q}[x] \,|\, \deg f(x) \le n\}$. Επειδή κάθε $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Q}_n[x]$ καθορίζεται μοναδικά από τη διατεταγμένη n+1 - άδα $(a_n, \ldots, a_0)$, υπάρχει 1-1 και επί αντιστοιχία μεταξύ των συνόλων $\mathbb{Q}_n[x]$ και $\underbrace{\mathbb{Q} \times \mathbb{Q} \times \ldots \times \mathbb{Q}}_{n+1 \text{ φορές}}$. Από αυτό έπεται ότι το $\mathbb{Q}_n[x]$ είναι αριθμήσιμο γιατί το $\mathbb{Q}$ είναι αριθμήσιμο. Επειδή $\mathbb{Q}[x] = \bigcup_{n=0,1,\ldots} \mathbb{Q}_n[x]$ και η ένωση αριθμήσιμου πλήθους αριθμήσιμων συνόλων είναι αριθμήσιμο, συμπεραίνουμε ότι το σύνολο $\mathbb{Q}[x]$ είναι αριθμήσιμο. Έστω $\overline{\mathbb{Q}}$ το σύνολο των μιγαδικών που είναι αλγεβρικοί πάνω από το $\mathbb{Q}$. Ξέρουμε ότι για κάθε μη μηδενικό $f(x) \in \mathbb{Q}[x]$ το σύνολο των ριζών $\{a \in \mathbb{C} \,|\, f(a) = 0\}$ είναι πεπερασμένο. Από

$$\overline{\mathbb{Q}} = \bigcup_{\substack{f(x) \in \mathbb{Q}[x] \\ f(x) \neq 0}} \{a \in \mathbb{C} \,|\, f(a) = 0\},$$

που είναι ένωση αριθμήσιμου πλήθους πεπερασμένων συνόλων, έπεται ότι σύνολο $\overline{\mathbb{Q}}$ είναι αριθμήσιμο. Επειδή το $\mathbb{C}$ είναι μη αριθμήσιμο, έχουμε $\overline{\mathbb{Q}} \neq \mathbb{C}$.

iii) Η επέκταση $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ είναι αλγεβρική γιατί κάθε στοιχείο του $\mathbb{Q}(\sqrt{2})$ έχει τη μορφή $a + b\sqrt{2}$, όπου $a, b \in \mathbb{Q}$, και το $a + b\sqrt{2}$ είναι ρίζα του $x^2 - 2ax + a^2 - 2b^2$ που έχει ρητούς συντελεστές.

Θεώρημα 2.2 *Κάθε πεπερασμένη επέκταση είναι αλγεβρική.*

Απόδειξη Έστω $F \subseteq K$ πεπερασμένη επέκταση βαθμού $n < \infty$ και $a \in K$. Τότε τα στοιχεία $1, a, a^2, \ldots, a^n$ του K είναι γραμμικά εξαρτημένα πάνω από το F. Συνεπώς υπάρχουν $c_i \in F$, όχι όλα 0, με $c_0 + c_1 a + \ldots + c_n a^n = 1$. Δηλαδή έχουμε $f(a) = 0$, όπου $f(x) = c_0 + c_1 x + \ldots + c_n x^n \in F[x]$ και $f(x) \neq 0$. Άρα το a είναι αλγεβρικό πάνω από το F.

Έστω $F \subseteq K$ επέκταση και $a, b \in K$ αλγεβρικά στοιχεία πάνω από το F. Τότε καθεμιά από τις επεκτάσεις που εμφανίζονται στην αλυσίδα

$$F \subseteq F(a) \subseteq F(a,b)$$

είναι αλγεβρική.

Πράγματι, από την Πρόταση 1.5 ii), $[F(a):F]=\deg Irr(a,F)$ και άρα η επέκταση $F\subseteq F(a)$ είναι αλγεβρική από το Θεώρημα 2.2.

Επίσης, $[F(a,b):F(a)]=\deg Irr(b,F(a))\le \deg Irr(b,F)$ λόγω της Πρότασης 1.5 iii). Άρα η $F(a)\subseteq F(a,b)$ είναι αλγεβρική. Από το Θεώρημα 1.7 έπεται ότι $[F(a,b)]=[F(a,b):F(a)][F(a):F]<\infty$ οπότε και η επέκταση $F\subseteq F(a,b)$ είναι αλγεβρική.

Με παρόμοιο συλλογισμό αποδεικνύεται το εξής αποτέλεσμα.

Πόρισμα 2.3 *Έστω $F\subseteq K$ επέκταση και $a_1,...,a_n\in K$ αλγεβρικά στοιχεία πάνω από το F. Τότε η επέκταση $F\subseteq F(a_1,...,a_n)$ είναι πεπερασμένη (και αλγεβρική).*

Πόρισμα 2.4 *Αν $F\subseteq K$ και $K\subseteq L$ είναι αλγεβρικές επεκτάσεις, τότε η $F\subseteq L$ είναι αλγεβρική.*

Απόδειξη Έστω $a\in L$. Το a είναι αλγεβρικό πάνω από το K. Έστω $Irr(a,K)=x^n+a_{n-1}x^{n-1}+...+a_0$. Το a είναι αλγεβρικό πάνω από το $F(a_0,...,a_{n-1})$ και $[F(a_0,...,a_{n-1},a):F(a_0,...,a_{n-1})]<\infty$. Κάθε a_i είναι αλγεβρικό πάνω από το F και άρα η επέκταση $F\subseteq F(a_0,...,a_{n-1})$ είναι πεπερασμένη από το προηγούμενο πόρισμα. Συνεπώς

$$[F(a_0,...,a_{n-1},a):F]=[F(a_0,...,a_{n-1},a):F(a_0,...,a_{n-1})][F(a_0,...,a_{n-1}):F]<\infty$$

και η επέκταση $F\subseteq F(a_0,...,a_{n-1},a)$ είναι αλγεβρική από το Θεώρημα 2.2.

Πόρισμα 2.5 *Έστω $F\subseteq K$ επέκταση και E το υποσύνολο του K των στοιχείων που είναι αλγεβρικά πάνω από το F. Τότε το E είναι υπόσωμα του K και η επέκταση $F\subseteq E$ είναι αλγεβρική.*

Απόδειξη Αν $a,b\in E$, τότε η επέκταση $F\subseteq F(a,b)$ είναι αλγεβρική από το Πόρισμα 2.3. Επειδή τα $a+b, ab, a-b, ab^{-1}$ ($b\neq 0$ στην τελευταία σχέση) ανήκουν στο $F(a,b)$, είναι αλγεβρικά πάνω από το F οπότε ανήκουν στο E. Άρα το E είναι υπόσωμα του K.

Για $F=\mathbb{Q}$ και $K=\mathbb{C}$, το E του Πορίσματος 2.5 λέγεται το **σώμα των αλγεβρικών αριθμών** και θα το συμβολίζουμε με $\overline{\mathbb{Q}}$.

Παρατήρηση Η επέκταση $\mathbb{Q}\subseteq\overline{\mathbb{Q}}$ είναι παράδειγμα άπειρης αλγεβρικής επέκτασης. Πράγματι, για κάθε θετικό ακέραιο n έχουμε $\sqrt[n]{2}\in\overline{\mathbb{Q}}$ αφού το $\sqrt[n]{2}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$ ως ρίζα του $x^n-2\in\mathbb{Q}[x]$.

$$\begin{array}{c}\overline{\mathbb{Q}}\\ |\\ \mathbb{Q}(\sqrt[n]{2})\\ |\ \}\ n\\ \mathbb{Q}\end{array}$$

Από το Παράδειγμα 1.4 i) και την Πρόταση 1.5 ii) έπεται ότι $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]=n$. Από $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[n]{2})\subseteq\overline{\mathbb{Q}}$ έχουμε $[\overline{\mathbb{Q}}:\mathbb{Q}]\ge[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]=n$ για κάθε n. Άρα η επέκταση $\mathbb{Q}\subseteq\overline{\mathbb{Q}}$ είναι άπειρη.

Γεωμετρικές κατασκευές

Τα ακόλουθα προβλήματα της Ευκλείδειας Γεωμετρίας απασχόλησαν τους αρχαίους Έλληνες και μεταγενέστερους μαθηματικούς επί σειρά αιώνων. Οι πλήρεις απαντήσεις δόθηκαν το 19ο αιώνα.

- **Διπλασιασμός του κύβου**: Να κατασκευαστεί με κανόνα και διαβήτη ένας κύβος με διπλάσιο όγκο από δοσμένο κύβο.
- **Τριχοτόμηση γωνίας**: Να τριχοτομηθεί με κανόνα και διαβήτη δοσμένη γωνία.

- **Τετραγωνισμός του κύκλου**: Να κατασκευαστεί με κανόνα και διαβήτη τετράγωνο με εμβαδόν ίσο με το εμβαδόν δοσμένου κύκλου.

Χρησιμοποιώντας επεκτάσεις σωμάτων θα δείξουμε ότι οι παραπάνω κατασκευές είναι αδύνατες. Ξεκινάμε ορίζοντας αυστηρά ποιες 'κατασκευές επιτρέπονται'.

Ορισμοί

Έστω $S \subseteq \mathbb{R}^2$ ένα σύνολο σημείων του επιπέδου $\mathbb{R}^2$. Θεωρούμε τις εξής διαδικασίες.

1. (Κανόνας) Χάραξη ευθείας που διέρχεται από δύο σημεία του S.
2. (Διαβήτης) Χάραξη κύκλου με κέντρο σημείο του S και ακτίνα την απόσταση δύο σημείων του S.

Ένα σημείο του $\mathbb{R}^2$ λέγεται **κατασκευάσιμο από το S με 1 βήμα** αν είναι σημείο τομής ευθειών ή κύκλων που χαράχθηκαν με τις διαδικασίες 1 ή 2.

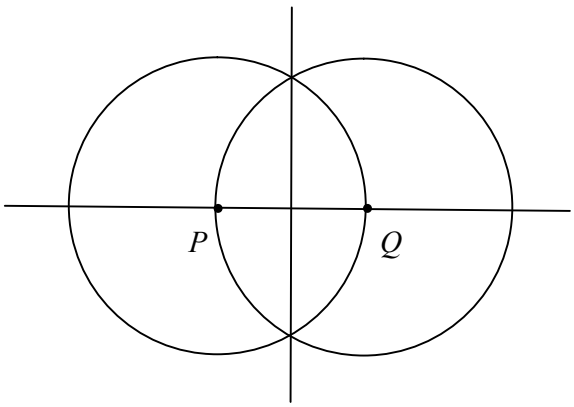
Ένα σημείο P του $\mathbb{R}^2$ λέγεται **κατασκευάσιμο από το S** αν υπάρχει πεπερασμένη ακολουθία σημείων

$$P_1, P_2, ..., P_n = P$$

τέτοια ώστε το P_1 είναι κατασκευάσιμο με 1 βήμα από το S και για κάθε $i = 2,..,n$ το P_i είναι κατασκευάσιμο με 1 βήμα από το σύνολο $S \cup \{P_1,...,P_{i-1}\}$.

Εφοδιάζουμε το επίπεδο $\mathbb{R}^2$ με ένα ορθογώνιο σύστημα συντεταγμένων με αρχή το O και θεωρούμε το σημείο I με συντεταγμένες $(1,0)$. Θέτουμε $S_0 = \{O, I\}$. Ένα σημείο P λέγεται **κατασκευάσιμο** αν είναι κατασκευάσιμο από το S_0.

Παράδειγμα Ας δούμε ένα απλό παράδειγμα που δείχνει ότι η συνήθης Ευκλείδεια κατασκευή του μέσου ευθυγράμμου τμήματος υλοποιείται σύμφωνα με αυτά που αναφέραμε πιο πάνω. Αν P, Q είναι διακεκριμένα κατασκευάσιμα σημεία, τότε το μέσο του ευθυγράμμου τμήματος PQ είναι κατασκευάσιμο. Φέρουμε την ευθεία PQ (κατασκευή τύπου 1). Φέρουμε δύο κύκλους με κέντρα P και Q και ακτίνα PQ (κατασκευές τύπου 2). Φέρουμε την ευθεία που διέρχεται από τα σημεία τομής των κύκλων (κατασκευή τύπου 1). Αυτή τέμνει το PQ στο μέσο του PQ.



Κατασκευάσιμα σημεία και επεκτάσεις

Θεωρούμε πεπερασμένη ακολουθία σημείων

$$P_1, P_2, ..., P_n = P$$

τέτοια ώστε το P_1 είναι κατασκευάσιμο με 1 βήμα από το S_0 και για κάθε $i = 2,..,n$ το P_i είναι κατασκευάσιμο με 1 βήμα από το σύνολο $S_0 \cup \{P_1,...,P_{i-1}\}$. Έστω (x_i, y_i) οι συντεταγμένες του P_i. Ορίζουμε μια ακολουθία διαδοχικών επεκτάσεων

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n \subseteq \mathbb{R}$$

ως εξής: $K_0 = \mathbb{Q}$ και επαγωγικά $K_i = K_{i-1}(x_i, y_i)$, $i = 1,..,n$.

Πρόταση 2.6 *Με τους προηγούμενους συμβολισμούς,* $\deg Irr(x_i, K_{i-1}) \le 2$ *και* $\deg Irr(y_i, K_{i-1}) \le 2$.

Απόδειξη Το σημείο P_i είναι σημείο τομής δύο ευθειών ή μίας ευθείας και ενός κύκλου ή δύο κύκλων. Ας δούμε αναλυτικά τη δεύτερη περίπτωση. Αφήνουμε τις άλλες δύο ως ασκήσεις.

Έχουμε μια ευθεία που διέρχεται από δύο σημεία A, B με συντεταγμένες $(a_1, a_2), (b_1, b_2)$ αντίστοιχα, τέτοιες ώστε $a_1, a_2, b_1, b_2 \in K_{i-1}$. Έχουμε ένα κύκλο με κέντρο σημείο C με συντεταγμένες (c_1, c_2) τέτοιες ώστε $c_1, c_2 \in K_{i-1}$ και ακτίνα r που είναι η απόσταση δύο σημείων D, E με συντεταγμένες $(d_1, d_2), (e_1, e_2)$ αντίστοιχα τέτοιες ώστε $d_1, d_2, e_1, e_2 \in K_{i-1}$. Από το Πυθαγόρειο θεώρημα, $r^2 = (d_1 - e_1)^2 + (d_2 - e_2)^2$ και επομένως $r^2 \in K_{i-1}$.

Ας υποθέσουμε ότι $a_1 \neq b_1$. Οι εξισώσεις της ευθείας και του κύκλου που αναφέραμε πριν είναι

$$y = \frac{b_2 - a_2}{b_1 - a_1}(x - a_1) + b_1,$$

$$(x - c_1)^2 + (y - c_2)^2 = r^2.$$

Αντικαθιστώντας την πρώτη σχέση στη δεύτερη προκύπτει

$$(x - c_1)^2 + (\frac{b_2 - a_2}{b_1 - a_1}(x - a_1) + b_1 - c_2)^2 = r^2$$

και άρα η πρώτη συντεταγμένη του P_i είναι ρίζα πολυωνύμου βαθμού 2 που έχει συντελεστές στο K_{i-1}. Τότε από τη σχέση $y = \frac{b_2 - a_2}{b_1 - a_1}(x - a_1) + b_1$, το ίδιο συμβαίνει για τη δεύτερη συντεταγμένη του P_i.

Αν $a_1 = b_1$, τότε έχουμε τις εξισώσεις

$$x = a_1,$$

$$(x - c_1)^2 + (y - c_2)^2 = r^2,$$

οπότε η πρώτη συντεταγμένη του P_i είναι στο K_{i-1} και η δεύτερη είναι ρίζα δευτεροβάθμιου πολυωνύμου με συντελεστές από το K_{i-1}.

Το κύριο αποτέλεσμα για κατασκευάσιμα σημεία είναι το ακόλουθο.

Θεώρημα 2.7 *Αν το σημείο* $P \in \mathbb{R}^2$ *είναι κατασκευάσιμο, τότε οι βαθμοί* $[\mathbb{Q}(x) : \mathbb{Q}]$ *και* $[\mathbb{Q}(y) : \mathbb{Q}]$ *είναι δυνάμεις του 2, όπου* (x, y) *είναι οι συντεταγμένες του* P.

Απόδειξη Αν το σημείο $P \in \mathbb{R}^2$ είναι κατασκευάσιμο, τότε υπάρχει πεπερασμένη ακολουθία σημείων

$$P_1, P_2, ..., P_n = P$$

τέτοια ώστε το P_1 είναι κατασκευάσιμο με 1 βήμα από το S_0 και για κάθε $i = 2, .., n$ το P_i είναι κατασκευάσιμο με 1 βήμα από το σύνολο $S_0 \cup \{P_1, ..., P_{i-1}\}$. Έστω (x_i, y_i) οι συντεταγμένες του P_i. Έχουμε μια ακολουθία διαδοχικών επεκτάσεων

$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n$, όπου $K_i = K_{i-1}(x_i, y_i)$ $i = 1, .., n$. Από την Πρόταση 2.6 έπεται ότι

$$[K_{i-1}(x_i) : K_{i-1}] = 1, 2$$

και όμοια,

$$[K_{i-1}(y_i) : K_{i-1}] = 1, 2.$$

Συνεπώς από το Θεώρημα 1.7 έχουμε

$$[K_i : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}] = 1, 2, 4.$$

Δηλαδή για κάθε i, το $[K_i : K_{i-1}]$ είναι δύναμη του 2. Επειδή

$$[K_n : \mathbb{Q}] = [K_n : K_{i-1}][K_{i-1} : K_{i-2}]...[K_1 : \mathbb{Q}]$$

έπεται ότι ο βαθμός $[K_n:\mathbb{Q}]$ είναι δύναμη του 2. Από

$$[K_n:\mathbb{Q}]=[K_n:\mathbb{Q}(x_n)][\mathbb{Q}(x_n):\mathbb{Q}]$$

παίρνουμε ότι το $[\mathbb{Q}(x_n):\mathbb{Q}]$ είναι δύναμη του 2. Όμοια και το $[\mathbb{Q}(y_n):\mathbb{Q}]$ είναι δύναμη του 2.

Τα κλασικά προβλήματα

1) *Διπλασιασμός του κύβου*: Δεν είναι δυνατό να κατασκευαστεί με κανόνα και διαβήτη κύβος όγκου 2 (Wantzel 1837).

Πράγματι, τοποθετώντας την ακμή στον άξονα των x, το σημείο $(a,0)$ θα ήταν κατασκευάσιμο, όπου $a^3=2$. Το πολυώνυμο x^3-2 είναι ανάγωγο πάνω από το $\mathbb{Q}$ (πχ από το κριτήριο του Eisenstein) οπότε $[\mathbb{Q}(a):\mathbb{Q}]=3$. Αυτό αντιβαίνει το Θεώρημα 2.7.

2) *Τριχοτόμηση γωνίας*: Δεν είναι δυνατό να τριχοτομηθεί τυχαία γωνία με κανόνα και διαβήτη (Wantzel, 1837).

Θα δείξουμε ότι η γωνία 60 μοιρών δεν τριχοτομείται με κανόνα και διαβήτη, ισοδύναμα το σημείο $(a,0)$ δεν είναι κατασκευάσιμο, όπου $a=\cos 20^o$. Η γνωστή τριγωνομετρική ταυτότητα $\cos(3\theta)=4\cos^3\theta-3\cos\theta$ δίνει ότι το a είναι ρίζα του $4x^3-3x-1/2$ δηλαδή του $8x^3-6x-1$. Αλλά εύκολα επαληθεύεται ότι το $8x^3-6x-1$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ (βλ. Πρόταση 0.1). Άρα $[\mathbb{Q}(\cos 20^o):\mathbb{Q}]=3$. Αυτό αντιβαίνει το Θεώρημα 2.7.

3) *Τετραγωνισμός του κύκλου*: Δεν είναι δυνατό να κατασκευαστεί με κανόνα και διαβήτη τετράγωνο εμβαδού π (Lindemann, 1882).

Πράγματι, σε αντίθετη περίπτωση το σημείο $(\sqrt{\pi},0)$ θα ήταν κατασκευάσιμο. Συνεπώς η επέκταση $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{\pi})$ θα ήταν αλγεβρική σύμφωνα με το Θεώρημα 2.7 και το Θεώρημα 2.1. Επειδή $\pi\in\mathbb{Q}(\sqrt{\pi})$, το π θα ήταν αλγεβρικό πάνω από το $\mathbb{Q}$. Ο Lindemann (1882) έδειξε ότι το π δεν είναι αλγεβρικό πάνω από το $\mathbb{Q}$.

Ασκήσεις 2

1.
   a. Έστω $a\in\mathbb{C}$. Δείξτε ότι η επέκταση $\mathbb{Q}\subseteq\mathbb{Q}(a)$ είναι αλγεβρική αν και μόνο αν η $\mathbb{Q}\subseteq\mathbb{Q}(a^2)$ είναι αλγεβρική.
   b. Αληθεύει ότι η επέκταση $\mathbb{Q}(\pi^3)\subseteq\mathbb{Q}(\pi)$ είναι αλγεβρική; Αν ναι, ποιο είναι το $Irr(\pi,\mathbb{Q}(\pi^3))$;
2. Θεωρούμε τις διαδοχικές επεκτάσεις

   $$\mathbb{Q}(\sqrt{3})\subseteq\mathbb{Q}(\sqrt[4]{3})\subseteq\mathbb{Q}(\sqrt[8]{3})\subseteq\ldots\subseteq\mathbb{Q}(\sqrt[2^n]{3})\subseteq\ldots$$

   και $F=\bigcup_{n=1}^{\infty}\mathbb{Q}(\sqrt[2^n]{3})$. Δείξτε ότι το F είναι σώμα και η επέκταση $\mathbb{Q}\subseteq F$ είναι αλγεβρική. Είναι πεπερασμένη;
3. Δείξτε ότι η επέκταση $F\subseteq K$ είναι πεπερασμένη αν και μόνο αν υπάρχουν $a_1,\ldots,a_n\in K$ αλγεβρικά στοιχεία πάνω από το F τέτοια ώστε $K=F(a_1,\ldots,a_n)$.
4. Έστω $a,b\in\mathbb{C}-\overline{\mathbb{Q}}$. Δείξτε ότι η επέκταση $\mathbb{Q}\subseteq\mathbb{Q}(a+b,ab)$ δεν είναι αλγεβρική.
5. Έστω F σώμα τέτοιο ώστε $\mathbb{Q}\subseteq F\subseteq\mathbb{Q}(\pi)$. Δείξτε ότι αν $[F:\mathbb{Q}]<\infty$, τότε $F=\mathbb{Q}$.
6. Συμπληρώστε την απόδειξη της Πρότασης 2.6.
7. Δείξτε ότι η κατασκευή κανονικού 9-γώνου με κανόνα και διαβήτη δεν είναι δυνατή.
8. Δείξτε ότι μια γωνία θ μπορεί να τριχοτομηθεί με κανόνα και διαβήτη αν και μόνο αν το πολυώνυμο $4x^3-3x-\cos\theta$ δεν είναι ανάγωγο πάνω από το $\mathbb{Q}(\cos\theta)$.

9. Έστω θ ακέραιος. Δείξτε ότι η γωνία θ μοιρών μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν και μόνο αν το θ είναι πολλαπλάσιο του 3.
10. Εξετάστε ποιες από τις επόμενες προτάσεις αληθεύουν.
    a. Οι επεκτάσεις $F \subseteq F(a)$ και $F \subseteq F(b)$ είναι αλγεβρικές αν και μόνο αν η επέκταση $F \subseteq F(a,b)$ είναι αλγεβρική.
    b. Έστω επέκταση $F \subseteq K$ και $a \in K - \{0\}$. Η επέκταση $F \subseteq F(a)$ είναι αλγεβρική αν και μόνο αν η επέκταση $F \subseteq F(a^{-1})$ είναι αλγεβρική.
    c. Έστω επέκταση $F \subseteq K$ και $a,b \in K$. Η επέκταση $F \subseteq F(a+b)$ είναι αλγεβρική αν και μόνο αν η επέκταση $F \subseteq F(a-b)$ είναι αλγεβρική.
    d. Έστω επέκταση $F \subseteq K$ και $a,b \in K$ τέτοια ώστε το a είναι αλγεβρικό πάνω από το F και το b δεν είναι αλγεβρικό πάνω από το F. Τότε το $a+b$ δεν είναι αλγεβρικό πάνω από το F.
11. Δείξτε ότι δεν είναι δυνατή η κατασκευή με κανόνα και διαβήτη ισοσκελούς τριγώνου με $p = 5$ και $h = 1,$ όπου p είναι η περίμετρος και h το μήκος του ύψους προς μια από τις ίσες πλευρές.

3. Σώμα ριζών

Βασικά σημεία

- Παραδείγματα σωμάτων ριζών.
- Ύπαρξη και 'μοναδικότητα' σώματος ριζών.
- Θεώρημα πρωταρχικού στοιχείου.
- Ιδιότητες σώματος ριζών (3.9, 3.10 και 3.11).

Ορισμός 3.1 *Έστω K επέκταση του F και $f(x) \in F[x]$ πολυώνυμο θετικού βαθμού. Το K λέγεται* ***σώμα ριζών*** *του $f(x)$ πάνω από το F αν υπάρχουν $a_1,...,a_n \in K$ τέτοια ώστε*

- $K = F(a_1,...,a_n)$ *και*
- *στο* $K[x]$ *ισχύει* $f(x) = c(x-a_1)(x-a_2)...(x-a_n)$, $c \in K$.

Παρατηρήσεις

i) Ένα σώμα ριζών του $f(x) \in F[x]$ πάνω από το F είναι ένα 'ελάχιστο' σώμα K ως προς τις ιδιότητες
   - $F \subseteq K$ και
   - το $f(x)$ αναλύεται πλήρως στο $K[x]$.

ii) Από το Πόρισμα 2.3 είναι σαφές ότι κάθε σώμα ριζών πάνω από το F είναι πεπερασμένη επέκταση του F και άρα αλγεβρική.

Παραδείγματα 3.2

i) Το $\mathbb{C}$ είναι σώμα ριζών του x^2+1 πάνω από το $\mathbb{R}$ αφού $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i,-i)$ και $x^2+1 = (x-i)(x+i)$.

ii) Το $\mathbb{Q}(\sqrt{2})$ είναι σώμα ριζών του x^2-2 πάνω από το $\mathbb{Q}$ αφού $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2},-\sqrt{2})$ και $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

iii) Το $\mathbb{Q}(i,\sqrt{2})$ είναι σώμα ριζών του x^2-2 πάνω από το $\mathbb{Q}(i)$. Επίσης, το $\mathbb{Q}(i,\sqrt{2})$ είναι σώμα ριζών του $(x^2+1)(x^2-2)$ πάνω από το $\mathbb{Q}$.

iv) Το $\mathbb{Q}(\sqrt{2},\sqrt{3})$ είναι σώμα ριζών του $x^4-5x^2+6 = (x^2-2)(x^2-3)$ πάνω από το $\mathbb{Q}$.
Επίσης, το $\mathbb{Q}(\sqrt{2},\sqrt{3})$ είναι σώμα ριζών του
$$x^4-10x^2+1 = (x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$$
πάνω από το $\mathbb{Q}$ αφού $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3},-\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3})$.

v) Το $\mathbb{Q}(\zeta_n)$ είναι σώμα ριζών του x^n-1 πάνω από το $\mathbb{Q}$, όπου $\zeta_n = \cos(2\pi/n)+i\sin(2\pi/n)$, αφού $\mathbb{Q}(\zeta_n) = \mathbb{Q}(1,\zeta_n,\zeta_n^{\,2},...,\zeta_n^{\,n-1})$ και $x^n-1 = (x-1)(x-\zeta_n)(x-\zeta_n^{\,2})...(x-\zeta_n^{\,n-1})$.

vi) Έστω $\rho = \sqrt[3]{5}$ και $\omega = (-1+i\sqrt{3})/2$. Το $K = \mathbb{Q}(\rho,\omega)$ είναι σώμα ριζών του x^3-5 πάνω από το $\mathbb{Q}$ αφού $x^3-5 = (x-\rho)(x-\rho\omega)(x-\rho\omega^2)$ και $\mathbb{Q}(\rho,\omega) = \mathbb{Q}(\rho,\rho\omega,\rho\omega^2)$. Επίσης, το $\mathbb{Q}(\rho,\omega)$ είναι σώμα ριζών του x^2+x+1 πάνω από το $\mathbb{Q}(\rho)$ αφού $x^2+x+1 = (x-\omega)(x-\omega^2)$.

Παρατήρηση 3.3 Έστω $F \subseteq E \subseteq K$ διαδοχικές επεκτάσεις και K είναι σώμα ριζών ενός $f(x) \in F[x]$. Τότε θεωρώντας $f(x) \in E[x]$, το K είναι σώμα ριζών του $f(x)$ πάνω από το E. Πράγματι, αν $K = F(a_1,...,a_n)$, τότε $K = E(a_1,...,a_n)$ αφού $E \subseteq K$.

$$\left.\begin{array}{l} K \\ | \\ E \\ | \\ F \end{array}\right\} \text{ σώμα ριζών } \Rightarrow \left.\begin{array}{l} K \\ | \\ E \\ | \\ F \end{array}\right\} \text{ σώμα ριζών}$$

Σημειώνουμε ότι το E δεν είναι αναγκαστικά σώμα ριζών πάνω από το F, βλ. άσκηση 3.6.

Θεώρημα 3.4 (ύπαρξης) *Έστω $f(x) \in F[x]$ βαθμού $n > 0$. Τότε υπάρχει σώμα ριζών K του $f(x)$ πάνω από το F με $[K : F] \le n!$.*

Απόδειξη Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι το $f(x)$ είναι μονικό. Χρησιμοποιούμε επαγωγή στο n. Για $n = 1$, έχουμε $f(x) = x - a$ και το F είναι σώμα ριζών του $f(x)$ πάνω από το F.
Έστω $n \ge 2$ και υποθέτουμε ότι το θεώρημα αληθεύει για κάθε πολυώνυμο του $F[x]$ βαθμού $n-1$.
Σύμφωνα με το Θεώρημα 1.12 υπάρχει επέκταση K του F όπου το $f(x)$ έχει ρίζα, έστω a. Έχουμε $f(x) = (x-a)g(x)$ για κάποιο $g(x) \in F(a)[x]$. Άρα $\deg g(x) = n-1$. Από την Πρόταση 1.5 έχουμε

$$[F(a) : F] \le \deg f(x) = n.$$

Από την επαγωγική υπόθεση, υπάρχει σώμα ριζών L του $g(x)$ πάνω από το $F(a)$ με $[L : F(a)] \le (n-1)!$.
Το L είναι σώμα ριζών του $f(x)$ πάνω από το F. Πράγματι, αν $L = F(a)(a_2, ..., a_n)$ και $g(x) = (x-a_2)...(x-a_n)$, τότε $L = F(a, a_2, ..., a_n)$ και $f(x) = (x-a)(x-a_2)...(x-a_n)$. Από το Θεώρημα 1.10,

$$[L : F] = [L : F(a)][F(a) : F] \le (n-1)!n = n!.$$

Το θεώρημα επέκτασης ισομορφισμών δίνει για σώματα ριζών το ακόλουθο αποτέλεσμα.

Λήμμα 3.5 *Έστω $\tau : F_1 \to F_2$ ισομορφισμός σωμάτων, K_1 ένα σώμα ριζών του $f(x) \in F_1[x]$ πάνω από το F_1 και K_2 ένα σώμα ριζών του $\tau(f(x)) \in F_2[x]$ πάνω από το F_2. Τότε υπάρχει ισομορφισμός $\sigma : K_1 \to K_2$ με $\sigma(c) = \tau(c)$ για κάθε $c \in F_1$.*

$$\begin{array}{ccc} K_1 & \xrightarrow{\sigma} & K_2 \\ | & & | \\ F_1 & \xrightarrow{\tau} & F_2 \end{array}$$

Απόδειξη Επαγωγή στο $n = \deg f(x)$. Αν $n = 1$, τότε $K_1 = F_1$ και $K_2 = F_2$. Ως σ μπορούμε να θέσουμε το τ. Έστω $n \ge 2$ και υποθέτουμε ότι το θεώρημα αληθεύει για κάθε $f(x) \in F_1[x]$ βαθμού $n-1$. Έστω $a \in K_1$ ρίζα ανάγωγου παράγοντα $p(x) \in F_1[x]$ του $f(x)$ και $b \in K_2$ ρίζα του $\tau(p(x)) \in F_2[x]$. Από το θεώρημα επέκτασης ισομορφισμών (Θεώρημα 1.9), υπάρχει ισομορφισμός $\sigma : F(a) \to F(b)$ που επεκτείνει τον τ και ικανοποιεί $\sigma(a) = b$.

$$\begin{array}{ccc} K_1 & \xrightarrow{\sigma} & K_2 \\ | & & | \\ F_1(a) & \xrightarrow{\sigma_1} & F_2(b) \\ | & & | \\ F_1 & \xrightarrow{\tau} & F_2 \end{array}$$

Έχουμε μια παραγοντοποίηση $f(x)=(x-a)g(x)$ στο $F_1(a)[x]$ και άρα $\sigma_1(f(x))=(x-b)\sigma_1(g(x))$ στο $F_2(b)[x]$. Επειδή το K_1 είναι σώμα ριζών του $f(x)$ πάνω από το F_1, το K_1 είναι σώμα ριζών του $g(x)$ πάνω από το $F_1(a)$. Όμοια το K_2 είναι σώμα ριζών του $\sigma_1(g(x))$ πάνω από το $F_2(b)$. Επειδή $\deg g(x)=n-1$, η επαγωγική υπόθεση δίνει την ύπαρξη ισομορφισμού $\sigma: K_1 \to K_2$ που επεκτείνει τον σ_1 και άρα επεκτείνει τον τ.

Θεωρώντας στο λήμμα την ειδική περίπτωση που $F_1=F_2=F$ και $\tau: F\to F$ είναι η ταυτοτική απεικόνιση $\tau=1_F$, προκύπτει το εξής.

Πόρισμα 3.6 (μοναδικότητα) *Κάθε δύο σώματα ριζών του $f(x)\in F[x]$ πάνω από το F είναι ισόμορφα.*

Θεώρημα πρωταρχικού στοιχείου

Αν μια επέκταση $F\subseteq K$ είναι πεπερασμένη, τότε υπάρχουν στοιχεία $\alpha_1,...,\alpha_n\in K$ με $K=F(\alpha_1,...,\alpha_n)$ (βλ. άσκηση 2.3). Στην περίπτωση που η χαρακτηριστική του F είναι 0 έχουμε το ακόλουθο αποτέλεσμα που θα χρησιμοποιηθεί συχνά σε επόμενες ενότητες.

Θεώρημα 3.7 (πρωταρχικού στοιχείου) *Αν $F\subseteq K$ είναι πεπερασμένη επέκταση και η χαρακτηριστική του F είναι 0, τότε υπάρχει $\theta\in K$ με $K=F(\theta)$.*

Απόδειξη Εφόσον $[K:F]<\infty$, υπάρχουν $\alpha_1,...,\alpha_n\in K$ με $K=F(\alpha_1,...,\alpha_n)$. Επομένως αρκεί να αποδείξουμε ότι: αν $K=F(a,b)$, τότε υπάρχει $\theta\in K$ με $K=F(\theta)$. (Το ζητούμενο προκύπτει από διαδοχική εφαρμογή της ανωτέρω συνεπαγωγής).

Έστω $p(x)=Irr(a,F)$ και $q(x)=Irr(b,F)$. Έστω $a_1=a,a_2,...,a_m$ οι ρίζες του $p(x)$ στο L και $b_1=b,b_2,...,b_n$ οι ρίζες του $q(x)$ στο L, όπου L σώμα ριζών του $p(x)q(x)$ πάνω από το K.

Τα b_j είναι διαφορετικά ανά δύο λόγω της Πρότασης 0.8. Θεωρούμε τα στοιχεία

$$\frac{a_i-a_1}{b_1-b_j}\in L \qquad (1)$$

όπου $j\neq 1$. Επειδή τα στοιχεία στην (1) είναι πεπερασμένου πλήθους και το F είναι άπειρο σύνολο (είναι σώμα χαρακτηριστικής 0), υπάρχει $c\in F-\{0\}$ με c διάφορο από κάθε στοιχείο στη (1). Θέτουμε

$$\theta=a+cb. \qquad (2)$$

Θα αποδείξουμε ότι $F(a,b)=F(\theta)$. Η σχέση $F(\theta)\subseteq F(a,b)$ είναι προφανής. Αρκεί να δείξουμε ότι $a,b\in F(\theta)$ και για τούτο αρκεί να δείξουμε ότι $b\in F(\theta)$ λόγω της (2).

Θεωρούμε το πολυώνυμο

$$r(t)=p(\theta-ct)\in F(\theta)[t].$$

Ισχύει $r(b)=p(\theta-cb)=p(a)=0$. Έτσι το b είναι κοινή ρίζα των πολυωνύμων $r(t)\in F(\theta)[t]$ και $q(t)\in F[t]\subseteq F(\theta)[t]$. Επομένως

$$Irr(b,F(\theta))\,|\,r(t) \quad \text{και} \quad Irr(b,F(\theta))\,|\,q(t). \qquad (3)$$

Ισχυρισμός. Τα πολυώνυμα $r(t)$ και $q(t)$ έχουν ακριβώς μια κοινή ρίζα στο L.

Πράγματι, αν $\rho\in L$ είναι ρίζα του $r(t)$, το $\theta-c\rho\in L$ είναι ρίζα του $p(t)$ και άρα για κάποιο s,

$$\theta-c\rho=a_s.$$

Αν $\rho=b_t$, τότε $a+cb-cb_t=a_s$ και ο ορισμός του c δίνει $\rho=b$.

Από τον ισχυρισμό, την (3) και το γεγονός ότι τα b_j είναι διαφορετικά ανά δύο, έπεται ότι το πολυώνυμο $Irr(b,F(\theta))$ είναι πρωτοβάθμιο. Άρα $b\in F(\theta)$.

Παράδειγμα Έστω $F=\mathbb{Q}(\sqrt{3},\sqrt{7})$. Με το συμβολισμό της προηγούμενης απόδειξης έχουμε

$$a_1=\sqrt{3},\ a_2=-\sqrt{3},$$
$$b_1=\sqrt{7},\ b_2=-\sqrt{7},$$
$$\frac{a_i-a_1}{b_1-b_2}=0,\ -\frac{\sqrt{3}}{\sqrt{7}}.$$

Από την απόδειξη έπεται ότι για κάθε $c\in\mathbb{Q}-\{0,-\frac{\sqrt{3}}{\sqrt{7}}\}$, δηλαδή για κάθε $c\in\mathbb{Q}-\{0\}$, ισχύει $\mathbb{Q}(\sqrt{3},\sqrt{7})=\mathbb{Q}(\sqrt{3}+c\sqrt{7})$. Για παράδειγμα, μπορούμε να θέσουμε $c=1$, οπότε $\mathbb{Q}(\sqrt{3},\sqrt{7})=\mathbb{Q}(\sqrt{3}+\sqrt{7})$.

Σημείωση Το συμπέρασμα του θεωρήματος 3.7 ισχύει κάτω από ασθενέστερες υποθέσεις. Δύο περιπτώσεις είναι οι εξής.

i) Έστω $F\subseteq K$ πεπερασμένη επέκταση όπου το F είναι άπειρο σώμα τέτοιο ώστε για κάθε $a\in K$ το $Irr(a,F)$ δεν έχει πολλαπλή ρίζα σε οποιοδήποτε σώμα ριζών του. Τότε υπάρχει $\theta\in K$ με $K=F(\theta)$.
Η απόδειξη είναι ουσιαστικά ίδια με αυτή που είδαμε.

ii) Έστω $F\subseteq K$ επέκταση όπου τα F και K είναι πεπερασμένα σώματα. Τότε υπάρχει $\theta\in K$ με $K=F(\theta)$.
Αυτό έπεται από το γεγονός ότι η πολλαπλασιαστική ομάδα κάθε πεπερασμένου σώματος είναι κυκλική. Θα δούμε μια απόδειξη στην Ενότητα 9.

Στο μάθημα θα αποδείξουμε το θεμελιώδες θεώρημα της θεωρίας Galois για α) σώματα ριζών χαρακτηριστικής 0 και β) πεπερασμένα σώματα. Στην απόδειξη του α) θα χρησιμοποιήσουμε το Θεώρημα 3.7.

Ιδιότητες σώματος ριζών

Έστω $K=F(a_1,...,a_n)$ σώμα ριζών του $f(x)\in F[x]$ πάνω από το F, όπου

$$f(x)=c(x-a_1)(x-a_2)...(x-a_n),$$

L επέκταση του K και $\sigma:K\to L$ μονομορφισμός σωμάτων τέτοιος ώστε $\sigma(c)=c$ για κάθε $c\in F$. Από $f(a_i)=0$ παίρνουμε

$$0=\sigma(0)=\sigma(f(a_i))=f(\sigma(a_i)),$$

δηλαδή το $\sigma(a_i)$ είναι ρίζα του $f(x)$ στο L και άρα το $\sigma(a_i)$ είναι ένα από τα $a_1,...,a_n$. Άρα

$$\sigma(K)\subseteq K,$$

γιατί κάθε στοιχείο του K έχει τη μορφή $h(a_1,...,a_n)$, όπου $h(x_1,...,x_n)\in F[x_1,...,x_n]$ (βλ. Παρατήρηση ii) μετά τα Παραδείγματα 1.6), και $\sigma(h(a_1,...,a_n))=h(\sigma(a_1),...,\sigma(a_n))\in K$.

Από $\sigma(K)\subseteq K$ έπεται ότι $\sigma(K)=K$ αφού $[\sigma(K):F]=[K:F]<\infty$ (η τελευταία ισότητα ισχύει αφού η απεικόνιση σ είναι μονομορφιμός F-διανυσματικών χώρων). Συνεπώς έχουμε το εξής αποτέλεσμα.

Λήμμα 3.8 *Έστω K σώμα ριζών του $f(x)\in F[x]$ πάνω από το F, L επέκταση του K και $\sigma:K\to L$ μονομορφισμός σωμάτων τέτοιος ώστε $\sigma(c)=c$ για κάθε $c\in F$. Τότε $\sigma(K)\subseteq K$ και άρα $\sigma(K)=K$.*

Σύμφωνα με τον ορισμό, αν K είναι σώμα ριζών του $f(x)\in F[x]$ πάνω από το F, τότε το $f(x)$ αναλύεται πλήρως στο $K[x]$. Θα δούμε τώρα την ιδιαίτερα ενδιαφέρουσα ιδιότητα ότι κάθε ανάγωγο πολυώνυμο του $F[x]$ που έχει μια ρίζα στο K αναλύεται πλήρως στο K. Δηλαδή ένα ανάγωγο πολυώνυμο του $F[x]$ ή δεν έχει ρίζα στο K ή αναλύεται πλήρως στο K.

Θεώρημα 3.9 *Έστω K σώμα ριζών πάνω από το F και $p(x)\in F[x]$ ανάγωγο στο $F[x]$. Αν το $p(x)$ έχει μία ρίζα στο K, τότε το $p(x)$ αναλύεται πλήρως στο $K[x]$.*

Απόδειξη Έστω $a \in K$ ρίζα του $p(x)$. Έστω L ένα σώμα ριζών του $p(x)$ πάνω από το K και $b \in L$ μια ρίζα του $p(x)$. Θα δείξουμε ότι $b \in K$.

Από το Θεώρημα 1.9 υπάρχει ισομορφισμός $\tau : F(a) \to F(b)$ που επεκτείνει την ταυτοτική απεικόνιση $1_F : F \to F$. Το K είναι σώμα ριζών του $f(x)$ πάνω από το $F(a)$ σύμφωνα με την Παρατήρηση 3.3. Επίσης το $K(b)$ είναι σώμα ριζών του $f(x)$ πάνω από το $F(b)$ γιατί αν $K = F(a_1,...,a_n)$, τότε $K(b) = F(a_1,...,a_n,b) = F(b)(a_1,...,a_n)$. Από το Λήμμα 3.5 υπάρχει ισομορφισμός $\sigma : K \to K(b)$ που επεκτείνει τον τ.

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K(b) \\ | & & | \\ F(a) & \xrightarrow{\tau} & F(b) \\ | & & | \\ F & \xrightarrow{1_F} & F \end{array}$$

Συνεπώς η σύνθεση $K \xrightarrow{\sigma} K(b) \subseteq L$ είναι μονομορφισμός και ο περιορισμός της στο F είναι η ταυτοτική απεικόνιση. Από το Λήμμα 3.7 έχουμε $\sigma(K) \subseteq K$, δηλαδή $K(b) \subseteq K$. Άρα $b \in K$.

Η προηγούμενη ιδιότητα χαρακτηρίζει τα σώματα ριζών, βλ. άσκηση 3.7 για την ακριβή διατύπωση.

Παραδείγματα

- $K = \mathbb{Q}(\sqrt[3]{5})$ δεν είναι σώμα ριζών πολυωνύμου πάνω από το $\mathbb{Q}$. Σε αντίθετη περίπωση το $x^3 - 5$, που είναι ανάγωγο πάνω από το $\mathbb{Q}$ και έχει ρίζα στο K, θα αναλυόταν πλήρως στο $K[x]$, άτοπο αφού το $x^3 - 5$ έχει μη πραγματική ρίζα και $K \subseteq \mathbb{R}$.
- Το $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ δεν περιέχει ρίζα του $f(x) = x^4 + 4x + 2$. Πράγματι, το K είναι σώμα ριζών πάνω από το $\mathbb{Q}$ (του πολυωνύμου $(x^2-2)(x^2-3)(x^2-5)$). Το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ σύμφωνα με το κριτήριο του Eisenstein για $p = 2$. Η παράγωγος του $f(x)$ είναι $4x^3 + 4$ που σημαίνει ότι η συνάρτηση $f : \mathbb{R} \to \mathbb{R}$ έχει το πολύ ένα τοπικό ακρότατο. Θεωρώντας τη γραφική παράσταση της συνάρτησης f συμπεραίνουμε ότι το πολυώνυμο $f(x)$ έχει μη πραγματική ρίζα. Από το Θεώρημα 3.9, αν κάποια ρίζα του $f(x)$ ήταν στο K, τότε όλες οι ρίζες του $f(x)$ θα ήταν στο K, πράγμα που δεν ισχύει αφού $K \subseteq \mathbb{R}$.

Στην ειδική περίπτωση που η χαρακτηριστική του F είναι 0 παίρνουμε το εξής αποτέλεσμα.

Πόρισμα 3.10 *Έστω K σώμα ριζών πάνω από το F. Αν η χαρακτηριστική του F είναι 0, τότε υπάρχει $a \in K$ τέτοιο ώστε $K = F(a)$ και το K είναι σώμα ριζών του $Irr(a,F)$ πάνω από το F.*

Απόδειξη Επειδή $[K : F] < \infty$ και η χαρακτηριστική του F είναι 0, από το Θεώρημα 3.7 υπάρχει $a \in K$ με $K = F(a)$. Το $Irr(a,F)$ αναλύεται πλήρως στο $K[x]$ σύμφωνα με το Θεώρημα 3.9. Άρα το K είναι σώμα ριζών του $Irr(a,F)$ πάνω από το F.

Παράδειγμα Το $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ είναι σώμα ριζών του $(x^2-2)(x^2-3) = x^4 - 5x^2 + 6$ πάνω από το $\mathbb{Q}$. Επειδή $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ (βλ. το παράδειγμα πριν το Θεώρημα 1.1), το Θεώρημα 3.9 δίνει ότι το K είναι σώμα ριζών του $p(x) = Irr(\sqrt{2} + \sqrt{3}, \mathbb{Q})$. Ισχύει $Irr(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$ (άσκηση).

Από το Λήμμα 3.5 προκύπτει η ακόλουθη ιδιότητα σωμάτων ριζών που, όπως θα δούμε στις Ενότητες 4 και 5, είναι ιδιαίτερα σημαντική για την απόδειξη του θεμελιώδους θεωρήματος της θεωρίας Galois.

Πόρισμα 3.11 *Έστω K σώμα ριζών του $f(x)\in F[x]$ πάνω από το F και $a,b\in K$. Τότε οι ακόλουθες προτάσεις είναι ισοδύναμες.*

- *Υπάρχει ισομορφισμός σωμάτων $\sigma: K\to K$ τέτοιος ώστε $\sigma(a)=b$ και $\sigma(c)=c$ για κάθε $c\in F$.*
- $Irr(a,F)=Irr(b,F)$.

Απόδειξη Έστω ότι υπάρχει ισομορφισμός σωμάτων $\sigma: K\to K$ τέτοιος ώστε $\sigma(a)=b$ και $\sigma(c)=c$ για κάθε $c\in F$. Επειδή το πολυώνυμο $p(x)=Irr(a,F)$ έχει συντελεστές στο F, παίρνουμε

$$p(b)=p(\sigma(a))=\sigma(p(a))=\sigma(0)=0.$$

Επειδή το $p(x)$ είναι ανάγωγο και έχει ρίζα το b έχουμε $p(x)=Irr(b,F)$. [Εδώ δεν χρειάστηκε ότι το K είναι σώμα ριζών πάνω από το F.]

Αντίστροφα, έστω $Irr(a,F)=Irr(b,F)$. Από το Πόρισμα 1.10 υπάρχει ισομορφισμός $\tau: F(a)\to F(b)$ που επεκτείνει την ταυτοτική απεικόνιση $F\to F$ και στέλνει το a στο b. Το ζητούμενο προκύπτει από το Λήμμα 3.5 (για $F_1=F(a), F_2=F(b), K_1=K_2=K, \tau=\tau$). [Παρόμοιο επιχείρημα είδαμε στην απόδειξη του Θεωρήματος 3.9].

Το νόημα της προηγούμενου πορίσματος είναι ότι για κάθε δύο συζυγή στοιχεία a,b σε ένα σώμα ριζών K πάνω από το F, υπάρχει ισομορφισμός $K\to K$ που στέλνει το a στο b και διατηρεί το F σημειακά σταθερό.

Παραδείγματα 3.12

i) Έστω $\rho=\sqrt[3]{5}$ και $\omega=(-1+i\sqrt{3})/2$. Το $K=\mathbb{Q}(\rho,\omega)$ είναι σώμα ριζών του x^3-5 πάνω από το $\mathbb{Q}$, όπως είδαμε στο Παράδειγμα 3.2 vi). Έστω $b\in K$. Από το Πόρισμα 3.11, υπάρχει ισομορφισμός $\sigma: K\to K$ με $\sigma(\rho)=b$ και $\sigma(c)=c$ για κάθε $c\in\mathbb{Q}$ αν και μόνο αν το b είναι ρίζα του $Irr(\rho,\mathbb{Q})=x^3-5$ δηλαδή αν και μόνο αν $b\in\{\rho,\rho\omega,\rho\omega^2\}$.

ii) Θα περιγράψουμε το σώμα ριζών K του $f(x)=x^4-10x^2+1$ στο $\mathbb{C}$ πάνω από το $\mathbb{Q}$ και θα βρούμε τους ισομορφισμούς σωμάτων $K\to K$.

Αν $\alpha\in\mathbb{C}$ είναι ρίζα του $f(x)$, τότε $\alpha^2=\dfrac{10\pm\sqrt{10^2-4}}{2}=5\pm2\sqrt{6}$. Άρα οι ρίζες του $f(x)$ στο $\mathbb{C}$ είναι οι πραγματικοί άριθμοί $\alpha=\sqrt{5+2\sqrt{6}}$, $\beta=\sqrt{5-2\sqrt{6}}$, $-\alpha,-\beta$. Άρα $K=\mathbb{Q}(\alpha,\beta)$. Όμως παρατηρούμε ότι $\alpha\beta=1$ και επομένως $K=\mathbb{Q}(\alpha)$. Αφήνουμε ως άσκηση την απόδειξη ότι το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$. (Ένας τρόπος είναι όπως στο παράδειγμα μετά το Λήμμα 0.2.) Συνεπώς $Irr(\alpha,\mathbb{Q})=f(x)$ και οι ρίζες του είναι οι $\alpha,\beta,-\alpha,-\beta$. Αν $\sigma: K\to K$ είναι ισομορφισμός σωμάτων, τότε όπως ξέρουμε $\sigma(c)=c$ για κάθε $c\in\mathbb{Q}$. Αυτό σημαίνει ότι ο σ καθορίζεται από την εικόνα $\sigma(\alpha)$. Από το Πόρισμα 3.11 έπεται όλοι οι ισομορφισμοί $K\to K$ είναι οι ακόλουθοι

$$\sigma_1: K\to K, \sigma_1(\alpha)=\alpha,$$
$$\sigma_2: K\to K, \sigma_2(\alpha)=\beta,$$
$$\sigma_3: K\to K, \sigma_3(\alpha)=-\alpha,$$
$$\sigma_4: K\to K, \sigma_4(\alpha)=-\beta.$$

Σημείωση. Επειδή $\sqrt{5+2\sqrt{6}}=\sqrt{2}+\sqrt{3}$ έχουμε $K=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

iii) Έστω $f(x)=x^3+x+1\in\mathbb{Z}_2[x]$ και a ρίζα του $f(x)$ σε επέκταση του $\mathbb{Z}_2$ σύμφωνα με το Θεώρημα 1.12. Θα δείξουμε ότι το $\mathbb{Z}_2(a)$ είναι σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Z}_2$ και θα βρούμε όλους τους ισομορφισμούς σωμάτων $\mathbb{Z}_2(a)\to\mathbb{Z}_2(a)$.

Επειδή το $f(x)$ είναι τρίτου βαθμού και δεν έχει ρίζα στο $\mathbb{Z}_2$, είναι ανάγωγο στο $\mathbb{Z}_2[x]$ και επομένως $Irr(a,\mathbb{Z}_2)=x^3+x+1$.

Το a^2 είναι ρίζα του $f(x)$ αφού $f(a^2)=f(a)^2=0$ σύμφωνα με την άσκηση 3.10 ή με έναν απευθείας υπολογισμό. Ομοίως το a^4 είναι ρίζα του $f(x)$.

Τα στοιχεία a,a^2,a^4 είναι ανά δύο διαφορετικά. Ένας τρόπος να το δούμε αυτό είναι με απευθείας υπολογισμό, για παράδειγμα αν $a^2=a^4$, τότε $a=0$ ή $a^2=1$. Η πρώτη περίπτωση αποκλείεται γιατί το 0 δεν είναι ρίζα του $f(x)$. Και η δεύτερη περίπτωση αποκλείεται, γιατί από $a^2=1$ παίρνουμε $a^3=a$ και άρα $f(a)=a^3+a+1=1\neq 0$. Ένας άλλος τρόπος είναι να παρατηρήσουμε ότι τα $1,a,a^2$ είναι βάση του $\mathbb{Z}_2(a)$ ως $\mathbb{Z}_2$-διανυσματικού χώρου σύμφωνα με την Πρόταση 1.5 και $a^4=aa^3=a(a+1)=a^2+a$. Άρα τα a,a^2,a^4 είναι ανά δύο διαφορετικά.

Από τα παραπάνω έπεται ότι $f(x)=(x-a)(x-a^2)(x-a^4)$. Άρα το $\mathbb{Z}_2(a,a^2,a^4)$ είναι σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Z}_2$. Παρατηρούμε ότι $\mathbb{Z}_2(a,a^2,a^4)=\mathbb{Z}_2(a)$.

Από το Πόρισμα 3.11 έπεται όλοι οι ισομορφισμοί $\mathbb{Z}_2(a)\to\mathbb{Z}_2(a)$ είναι οι ακόλουθοι

$$\sigma_1:\mathbb{Z}_2(a)\to\mathbb{Z}_2(a),\ \sigma_1(a)=a,$$
$$\sigma_2:\mathbb{Z}_2(a)\to\mathbb{Z}_2(a),\ \sigma_2(a)=a^2,$$
$$\sigma_3:\mathbb{Z}_2(a)\to\mathbb{Z}_2(a),\ \sigma_3(a)=a^4.$$

Ασκήσεις 3

1. Ποια από τα ακόλουθα σώματα είναι σώματα ριζών πάνω από το $\mathbb{Q}$;
   a. $\mathbb{Q}(\sqrt{3})$
   b. $\mathbb{Q}(\sqrt{3},i)$
   c. $\mathbb{Q}(\sqrt[3]{3})$
   d. $\mathbb{Q}(\sqrt[3]{3},i\sqrt{2})$.
2. Στις ακόλουθες περιπτώσεις να βρεθεί ο βαθμός του σώματος ριζών του πολυωνύμου πάνω από το σώμα F.
   a. $(x^2-2)(x^2-1),\quad F=\mathbb{Q}$.
   b. $(x^2-2)(x^2+1),\quad F=\mathbb{Q}$.
   c. $x^2-2,\quad F=\mathbb{Q}(\sqrt{3})$.
   d. $x^3-2,\quad F=\mathbb{Q}$.
   e. $x^3-2,\quad F=\mathbb{Q}(i\sqrt{3})$.
3. Να βρεθεί το σώμα ριζών $K\subseteq\mathbb{C}$ του x^4-8x^2+15 πάνω από το $\mathbb{Q}$. Στη συνέχεια να βρεθεί $a\in K$ τέτοιο ώστε $K=\mathbb{Q}(a)$.
4. Δείξτε ότι το σώμα $\mathbb{Q}(i,\sqrt{2})$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$ για καθένα από τα εξής πολυώνυμα
   a. x^4-2.
   b. x^4+2 .
   c. x^8-1.
5. Έστω επέκταση $F\subseteq K$ με $[K:F]=2$. Δείξτε ότι το K είναι σώμα ριζών πάνω από το F.
6. Θεωρούμε διαδοχικές επεκτάσεις $F\subseteq E\subseteq K$.
   a. Δείξτε ότι αν το K είναι σώμα ριζών πάνω από το F, τότε το K είναι σώμα ριζών πάνω από το E.

b. Δώστε ένα παράδειγμα όπου το K είναι σώμα ριζών πάνω από το F αλλά το E δεν είναι σώμα ριζών πάνω από το F.

c. Δώστε ένα παράδειγμα όπου το K είναι σώμα ριζών πάνω από το E, το E είναι σώμα ριζών πάνω από το F, αλλά το K δεν είναι σώμα ριζών πάνω από το F.

7.

a. Έστω $F \subseteq K$ πεπερασμένη επέκταση που έχει την ιδιότητα: 'Κάθε ανάγωγο πολυώνυμο στο $F[x]$ που έχει ρίζα στο K αναλύεται πλήρως στο $K[x]$'. Δείξτε ότι το K είναι σώμα ριζών πάνω από το F.

b. Χρησιμοποιώντας το προηγούμενο αποτέλεσμα δείξτε ότι η τομή δύο σωμάτων ριζών πάνω από το F είναι σώμα ριζών πάνω από το F.

8. Έστω K σώμα με $K \subseteq \mathbb{C}$ και $[K:\mathbb{Q}] < \infty$. Έστω ότι το K έχει την ιδιότητα: 'Για κάθε μονομορφισμό σωμάτων $\sigma : K \to \mathbb{C}$ ισχύει $\sigma(K) \subseteq K$'. Δείξτε ότι το K είναι σώμα ριζών πάνω από το $\mathbb{Q}$.

9. Έστω p πρώτος αριθμός. Το σώμα $\mathbb{Z}_p$ είναι σώμα ριζών του $x^p - x \in \mathbb{Z}_p[x]$ πάνω από το $\mathbb{Z}_p$.

10. Έστω p πρώτος αριθμός. Τότε για κάθε $f(x) \in \mathbb{Z}_p[x]$ ισχύει $f(x)^p = f(x^p)$.

11. Έστω $f(x) = x^3 - x + 1 \in \mathbb{Z}_3[x]$ και a ρίζα του $f(x)$ σε επέκταση του $\mathbb{Z}_3$.

a. Δείξτε ότι το $\mathbb{Z}_3(a)$ είναι σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Z}_3$.

b. Ποιο είναι το $Irr(a, \mathbb{Z}_3)$ και ποιες είναι οι ρίζες του στο $\mathbb{Z}_3(a)$;

c. Βρείτε όλους τους ισομορφισμούς σωμάτων $\mathbb{Z}_3(a) \to \mathbb{Z}_3(a)$.

12. *[1] Έστω p πρώτος αριθμός, F σώμα χαρακτηριστικής p και $f(x) = x^p - x - 1 \in F[x]$.

a. Έστω K επέκταση του F όπου το $f(x)$ έχει ρίζα. Δείξτε ότι το $f(x)$ αναλύεται πλήρως στο $K[x]$.

b. Δείξτε ότι αν το $f(x)$ δεν είναι ανάγωγο πάνω από το F, τότε αναλύεται πλήρως στο $F[x]$.

13. Έστω $a = \sqrt{1+\sqrt{7}}$ και $b = \sqrt{4+\sqrt{7}}$. Δείξτε τα εξής.

a. Το $\mathbb{Q}(a)$ δεν είναι σώμα ριζών πάνω από το $\mathbb{Q}$ και το πλήθος των ισομορφισμών $\mathbb{Q}(a) \to \mathbb{Q}(a)$ είναι ίσο με 2.

b. Το $\mathbb{Q}(b)$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$ και το πλήθος των ισομορφισμών $\mathbb{Q}(a) \to \mathbb{Q}(a)$ είναι ίσο με 4.

14. Εστω F σώμα, $f(x), p(x) \in F[x]$ και K σώμα ριζών του $f(x)$ πάνω από το F. Δείξτε ότι αν $\deg f(x) < \deg p(x)$, $\deg p(x)$ είναι πρώτος και $p(x)$ ανάγωγο πάνω από το F, τότε το $p(x)$ δεν έχει ρίζα στο K.

15. Έστω K σώμα ριζών πάνω από το $\mathbb{Q}$ τέτοιο ώστε το $\mathbb{Q}(i\sqrt{2})$ είναι το μοναδικό υπόσωμα του K βαθμού 2 πάνω από το $\mathbb{Q}$. Δείξτε ότι $\sqrt[3]{2} \notin K$.

16. Έστω $F \subseteq E \subseteq K$ διαδοχικές επεκτάσεις και $a \in K$ αλγεβρικό πάνω από το F. Δείξτε ότι οι συντελεστές του $Irr(a, E)$ είναι αλγεβρικοί πάνω από το F.

17. Θεωρούμε γνωστό ότι το π και το e δεν είναι αλγεβρικά πάνω από το $\mathbb{Q}$. Έστω $F = \mathbb{Q}(\pi)$, $p(x) = x^3 + \pi x + 6 \in F[x]$ και $K \subseteq \mathbb{C}$ το σώμα ριζών του $p(x)$ πάνω από F.

a. Δείξτε ότι $[K:F] = 6$.

b. Δείξτε ότι το K είναι ισόμορφο με το σώμα ριζών στο $\mathbb{C}$ του $x^3 + ex + 6$ πάνω από το $\mathbb{Q}(e)$.

18. Εξετάστε ποιες από τις επόμενες προτάσεις αληθεύουν.

a. Υπάρχει ισομορφισμός $\mathbb{Q}$ - διανυσματικών χώρων $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$.

b. Υπάρχει ισομορφισμός σωμάτων $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$.

[1] Με * σημειώνονται οι ασκήσεις που ίσως είναι πιο απαιτητικές.

c. Αν $f(x) \in \mathbb{Q}[x]$ είναι θετικού βαθμού, τότε τα σώματα ριζών στο $\mathbb{C}$ των πολυωνύμων $f(x), f(x)^2, f(x+1/2)$ είναι ίσα.

d. Υπάρχουν τουλάχιστον 9 διαφορετικοί μονομορφισμοί σωμάτων $\mathbb{Q}(\sqrt{2},\sqrt{3},i) \to \mathbb{C}$.

e. Υπάρχει μοναδικό υπόσωμα του $\mathbb{C}$ που είναι ισόμορφο με το $\mathbb{Q}(\sqrt{2},\sqrt{3},i)$.

f. Υπάρχει μοναδικό υπόσωμα του $\mathbb{C}$ που είναι ισόμορφο με το $\mathbb{Q}(\sqrt[3]{2})$.

4. Η ομάδα Galois

Βασικά σημεία

- Παραδείγματα ομάδων Galois.
- Σταθερό σώμα.
- Έστω K πεπερασμένη επέκταση του F και H υποομάδα της $Gal(K,F)$. Τότε $|H|=[K:FixH]$.
- Έστω K πεπερασμένη επέκταση του F και $G=Gal(K,F)$. Οι ακόλουθες προτάσεις είναι ισοδύναμες.
  - Το K είναι σώμα ριζών πάνω από το F.
  - $|G|=[K:F]$.
  - $F=FixG$.
- Η ομάδα Galois πολυωνύμου μεταθέτει τις ρίζες.

Έστω επέκταση $F\subseteq K$. Με $Gal(K,F)$ συμβολίζουμε το σύνολο των ισομορφισμών σωμάτων $\sigma:K\to K$ τέτοιων ώστε $\sigma(c)=c$ για κάθε $c\in F$. Τα στοιχεία του $Gal(K,F)$ ονομάζονται F-αυτομορφισμοί του K.

Εύκολα αποδεικνύεται ότι το $Gal(K,F)$ είναι ομάδα με πράξη τη σύνθεση απεικονίσεων. Πράγματι, αν $\sigma,\tau\in Gal(K,F)$, τότε $\sigma\circ\tau\in Gal(K,F)$ καθώς

- για κάθε $a,b\in K$,
  $\sigma\circ\tau(ab)=\sigma(\tau(a)\tau(b))=(\sigma\circ\tau(a))(\sigma\circ\tau(b))$ και
  $\sigma\circ\tau(a+b)=\sigma(\tau(a)+\tau(b))=\sigma\circ\tau(a)+\sigma\circ\tau(b)$
- για κάθε $c\in F$,
  $\sigma\circ\tau(c)=\sigma(\tau(c))=\sigma(c)=c$, και
- η απεικόνιση $\sigma\circ\tau$ είναι 1-1 και επί ως σύνθεση 1-1 και επί απεικονίσεων.

Το ουδέτερο στοιχείο είναι η ταυτοτική απεικόνιση $1_K:K\to K, 1_K(a)=a$. Αν $\sigma\in Gal(K,F)$, τότε η απεικόνιση σ είναι 1-1 και επί και άρα έχουμε την αντίστροφη απεικόνιση $\sigma^{-1}:K\to K$, που ορίζεται από $\sigma^{-1}(a)=b\Leftrightarrow a=\sigma(b)$. Εύκολα επαληθεύεται ότι η απεικόνιση $\sigma^{-1}:K\to K$ είναι F-αυτομορφισμός του K (άσκηση), δηλαδή $\sigma^{-1}\in Gal(K,F)$.

Ορισμός 4.1 *Η ομάδα $Gal(K,F)$ λέγεται η **ομάδα Galois** της επέκτασης $F\subseteq K$ (ή η ομάδα Galois του K πάνω από το F).*

Παράδειγμα Έστω $\sigma:\mathbb{C}\to\mathbb{C}, \sigma(z)=\overline{z}$, όπου $\overline{z}$ είναι ο συζυγής του μιγαδικού z (δηλαδή $\overline{z}=a-bi$, αν $z=a+bi$, όπου $a,b\in\mathbb{R}$). Εύκολα επαληθεύεται ότι η σ είναι ισομορφισμός και $\sigma(c)=c$ για κάθε $c\in\mathbb{R}$. Άρα $\sigma\in Gal(\mathbb{C},\mathbb{R})$. Έστω $\tau\in Gal(\mathbb{C},\mathbb{R})$. Από τη σχέση $i^2=-1$ παίρνουμε

$$\tau(i^2)=\tau(-1)\Rightarrow\tau(i)^2=-1\Rightarrow\tau(i)\in\{i,-i\}.$$

- Αν $\tau(i)=i$, τότε για κάθε $a,b\in\mathbb{R}$ έχουμε $\tau(a+bi)=\tau(a)+\tau(b)\tau(i)=a+bi$, δηλαδή η απεικόνιση τ είναι η ταυτοτική απεικόνιση $1_{\mathbb{C}}:\mathbb{C}\to\mathbb{C}$.
- Αν $\tau(i)=-i$, τότε για κάθε $a,b\in\mathbb{R}$ έχουμε $\tau(a+bi)=\tau(a)+\tau(b)\tau(i)=a-bi=\sigma(a+bi)$, δηλαδή η τ είναι η σ που είδαμε πριν.

Άρα $Gal(\mathbb{C},\mathbb{R})=\{1_{\mathbb{C}},\sigma\}$.

Παρατηρήσεις

i) Ξέρουμε ότι αν K είναι σώμα χαρακτηριστικής 0, τότε κάθε ισομορφισμός $\sigma:K\to K$ ικανοποιεί τη σχέση $\sigma(c)=c$ για κάθε $c\in\mathbb{Q}$. Άρα στην περίπτωση αυτή έχουμε $Gal(K,\mathbb{Q})=Aut(K)$, όπου $Aut(K)$ είναι το σύνολο των ισομορφισμών $K\to K$.

ii) Αν έχουμε διαδοχικές επεκτάσεις $F \subseteq E \subseteq K$, είναι σαφές ότι $Gal(K,E) \subseteq Gal(K,F)$. Μάλιστα εύκολα αποδεικνύεται ότι η ομάδα $Gal(K,E)$ είναι υποομάδα της $Gal(K,F)$.

Πρόταση 4.2 *Έστω πεπερασμένη επέκταση* $F \subseteq K$.

i) *Έστω* $f(x) \in F[x]$ *και* $a \in K$. *Αν το* a *είναι ρίζα του* $f(x)$, *τότε για κάθε* $\sigma \in Gal(K,F)$, *το* $\sigma(a)$ *είναι ρίζα του* $f(x)$.

ii) *Έστω* $K = F(a_1,...,a_n)$ *και* $\sigma, \tau \in Gal(K,F)$. *Τότε* $\sigma = \tau \Leftrightarrow \sigma(a_i) = \tau(a_i)$ *για κάθε* $i = 1,...,n$. *Δηλαδή αν* $\sigma \in Gal(K,F)$, *τότε ο* σ *καθορίζεται πλήρως από τις εικόνες* $\sigma(a_1),...,\sigma(a_n)$.

iii) *Η ομάδα* $Gal(K,F)$ *είναι πεπερασμένη.*

Απόδειξη i) Έστω $f(a) = 0$ και $f(x) = a_n x^n + ... + a_1 x + a_0$, όπου $a_i \in F$. Χρησιμοποιώντας ότι ο σ είναι ομομορφισμός σωμάτων και $\sigma(c) = c$ για κάθε $c \in F$, έχουμε

$$\begin{aligned} 0 = \sigma(0) = \sigma(f(a)) = \\ = \sigma(a_n a^n + ... + a_1 a + a_0) = \\ = \sigma(a_n)\sigma(a)^n + ... + \sigma(a_1)\sigma(a) + \sigma(a_0) = \\ = a_n \sigma(a)^n + ... + a_1 \sigma(a) + a_0 = \\ = f(\sigma(a)). \end{aligned}$$

ii) Επειδή η επέκταση $F \subseteq K$ είναι πεπερασμένη, κάθε a_i είναι αλγεβρικό πάνω από το F. Από τη δεύτερη Παρατήρηση μετά την Πρόταση 1.6 ξέρουμε ότι κάθε στοιχείο a του $F(a_1,...,a_n)$ είναι της μορφής $a = h(a_1,..,a_n)$, όπου $h(x_1,...,x_n) \in F[x_1,...,x_n]$. Τότε

$$\begin{aligned} \sigma(a) = \sigma(h(a_1,..,a_n)) = h(\sigma(a_1),..,\sigma(a_n)) = \\ = h(\tau(a_1),..,\tau(a_n)) = \tau(h(a_1,..,a_n)) = \\ = \tau(a). \end{aligned}$$

iii) Επειδή η επέκταση $F \subseteq K$ είναι πεπερασμένη, υπάρχουν $a_1,...,a_n \in K$ με $K = F(a_1,...,a_n)$ σύμφωνα με την άσκηση 2.3. Από το i), για κάθε $\sigma \in Gal(K,F)$ το $\sigma(a_i)$ είναι ρίζα του $Irr(a_i,F)$. Συνεπώς το $\sigma(a_i)$ λαμβάνει πεπερασμένο πλήθος τιμών. Το ζητούμενο έπεται από το ii).

Παραδείγματα 4.3

i) Έστω $K = \mathbb{Q}(\sqrt[3]{2})$. Θα δείξουμε ότι $Gal(K,\mathbb{Q}) = \{1_K\}$.

Έχουμε $Irr(\sqrt[3]{2},\mathbb{Q}) = x^3 - 2$ και οι ρίζες του στο $\mathbb{C}$ είναι οι $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, όπου $\omega = (-1 + i\sqrt{3})/2$. Αν $\sigma \in Gal(K,\mathbb{Q})$, τότε $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. Επειδή $\sigma(\sqrt[3]{2}) \in K \subseteq \mathbb{R}$, παίρνουμε $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Επειδή $K = \mathbb{Q}(\sqrt[3]{2})$, έχουμε $\sigma = 1_K$ σύμφωνα με την Πρόταση 4.2 ii). Άρα $Gal(K,\mathbb{Q}) = \{1_K\}$.

ii) Έστω $K = \mathbb{Q}(a,b), a = \sqrt{2}, b = \sqrt{3}$. Θα βρούμε τα στοιχεία της $Gal(K,\mathbb{Q})$ σε εκπεφρασμένη μορφή και θα δείξουμε ότι $Gal(K,\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Από $a^2 = 2$ και $b^2 = 3$ έπεται ότι

$$\sigma(a) \in \{a, -a\} \text{ και } \sigma(b) \in \{b, -b\}$$

για κάθε $\sigma \in Gal(K,\mathbb{Q})$. Άρα $|Gal(K,\mathbb{Q})| \le 2 \cdot 2 = 4$ σύμφωνα με την Πρόταση 4.2 ii).

Θα δούμε τώρα ότι για καθεμιά από τις παραπάνω επιλογές των εικόνων $\sigma(a), \sigma(b)$ υπάρχει αντίστοιχος ισομορφισμός $\sigma \in Gal(K,\mathbb{Q})$. Ας δούμε αναλυτικά την κατασκευή του ισομορφισμού που αντιστοιχεί στις επιλογές $-a \in \{a, -a\}$ και $-b \in \{b, -b\}$.

Έχουμε $Irr(a,\mathbb{Q}) = Irr(-a,\mathbb{Q}) = x^2 - 2$. Από το Πόρισμα 1.13 έπεται ότι υπάρχει ισομορφισμός $\tau : \mathbb{Q}(a) \to \mathbb{Q}(a)$ με $\tau(a) = -a$. Έχουμε $Irr(b,\mathbb{Q}(a)) = Irr(-b,\mathbb{Q}(a)) = x^2 - 3$. Πράγματι, επειδή το b

είναι ρίζα του x^2-3 έχουμε $Irr(b,\mathbb{Q}(a))\big|x^2-3$. Αλλά $b\notin\mathbb{Q}(a)$ (βλ. παράδειγμα μετά το Θεώρημα 1.10). Άρα $Irr(b,\mathbb{Q}(a))=Irr(-b,\mathbb{Q}(a))=x^2-3$. Εφαρμόζοντας το Θεώρημα 1.12 συμπεραίνουμε ότι υπάρχει ισομορφισμός $\sigma:K\to K$ τέτοιος ώστε $\sigma(b)=-b$ και $\sigma(c)=\tau(c)$ για κάθε $c\in\mathbb{Q}(a)$. Συνεπώς έχουμε $\sigma(a)=-a$ και $\sigma(b)=-b$.

$$\begin{array}{ccc}\mathbb{Q}(a,b) & \xrightarrow[\substack{a\mapsto -a\\ b\mapsto -b}]{\sigma} & \mathbb{Q}(a,b)\\ | & & | \\ \mathbb{Q}(a) & \xrightarrow[a\mapsto -a]{\tau} & \mathbb{Q}(a)\\ | & & | \\ \mathbb{Q} & \xrightarrow{1_{\mathbb{Q}}} & \mathbb{Q}\end{array}$$

Επαναλαμβάνοντας την παραπάνω κατασκευή ισομορφισμών $K\to K$ για κάθε επιλογή ενός στοιχείου από το σύνολο $\{a,-a\}$ και ενός από το $\{b,-b\}$ παίρνουμε $\sigma_1,\sigma_2,\sigma_3,\sigma_4\in Gal(K,F)$ όπως περιγράφονται στον ακόλουθο πίνακα.

$Gal(K,\mathbb{Q})$	$\sigma_i(a)=\ldots$	$\sigma_i(b)=\ldots$
σ_1	a	b
σ_2	a	$-b$
σ_3	$-a$	b
σ_4	$-a$	$-b$

Από τα παραπάνω έπεται ότι $Gal(K,\mathbb{Q})=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$. Επειδή η $Gal(K,\mathbb{Q})$ έχει τάξη 4, είναι αβελιανή. Εύκολα επαληθεύεται ότι $\sigma_i^{\,2}=\sigma_1$ για κάθε i. Για παράδειγμα,

$$\sigma_4{}^2(a)=\sigma_4(\sigma_4(a))=\sigma_4(-a)=-(-a)=a$$

και όμοια $\sigma_4{}^2(b)=b$. Άρα $\sigma_4{}^2=\sigma_1$. Συνεπώς η ομάδα $Gal(K,\mathbb{Q})$ είναι ισόμορφη με τη $\mathbb{Z}_2\times\mathbb{Z}_2$.

iii) Έστω $\rho=\sqrt[3]{5}$, $\omega\in\mathbb{C}$ μια ρίζα του πολυωνύμου x^2+x+1 και $K=\mathbb{Q}(\rho,\omega)$. Θα βρούμε τα στοιχεία της $Gal(K,\mathbb{Q})$ και άλλων ομάδων Galois σε εκπεφρασμένη μορφή και θα δείξουμε ότι $Gal(K,\mathbb{Q})\simeq S_3$, όπου S_3 είναι η συμμετρική ομάδα των μεταθέσεων του $\{1,2,3\}$.

Οι ρίζες του x^3-5 στο $\mathbb{C}$ είναι οι $\rho,\rho\omega,\rho\omega^2$ και οι ρίζες του x^2+x+1 στο $\mathbb{C}$ είναι οι ω,ω^2. Από $\rho^3=2$ και $\omega^2=1$ έπεται ότι

$$\sigma(\rho)\in\{\rho,\rho\omega,\rho\omega^2\}\ \text{ και }\ \sigma(\omega)\in\{\omega,\omega^2\}$$

για κάθε $\sigma\in Gal(K,\mathbb{Q})$. Άρα $\left|Gal(K,\mathbb{Q})\right|\le 3\cdot 2=6$.

Εργαζόμενοι όπως στο παράδειγμα ii) κατασκευάζουμε 6 διαφορετικούς ισομορφισμούς $K\to K$ που περιγράφονται από τον παρακάτω πίνακα. (Στο Παράδειγμα 1.14 είδαμε αναλυτικά μία περίπτωση, την κατασκευή του σ_6 παρακάτω).

$Gal(K,\mathbb{Q})$	$\sigma_i(\rho)=\ldots$	$\sigma_i(\omega)=\ldots$
σ_1	ρ	ω
σ_2	ρ	ω^2
σ_3	$\rho\omega$	ω
σ_4	$\rho\omega$	ω^2
σ_5	$\rho\omega^2$	ω
σ_6	$\rho\omega^2$	ω^2

Άρα $Gal(K,\mathbb{Q})=\{\sigma_1,\ldots,\sigma_6\}$.

Παρατηρούμε ότι η $Gal(K,\mathbb{Q})$ δεν είναι αβελιανή. Πράγματι,

$$\sigma_2 \circ \sigma_3(\rho) = \sigma_2(\sigma_3(\rho)) = \sigma_2(\rho\omega) = \sigma_2(\rho)\sigma_2(\omega) = \rho\omega^2,$$
$$\sigma_3 \circ \sigma_2(\rho) = \sigma_3(\sigma_2(\rho)) = \sigma_3(\rho) = \rho\omega,$$

οπότε $\sigma_2 \circ \sigma_3 \neq \sigma_3 \circ \sigma_2$. Επειδή η ομάδα $Gal(K,\mathbb{Q})$ είναι τάξης 6 και μη αβελιανή, είναι ισόμορφη με τη συμμετρική ομάδα S_3.

Από τον παραπάνω πίνακα έπεται ότι

$$Gal(K,\mathbb{Q}(\omega)) = \{\sigma_1, \sigma_3, \sigma_5\},$$
$$Gal(K,\mathbb{Q}(\rho)) = \{\sigma_1, \sigma_2\},$$
$$Gal(K,\mathbb{Q}(\rho\omega)) = \{\sigma_1, \sigma_6\},$$
$$Gal(K,\mathbb{Q}(\rho\omega^2)) = \{\sigma_1, \sigma_4\}.$$

Για παράδειγμα, αν $\sigma \in Gal(K,\mathbb{Q})$, τότε

$$\sigma \in Gal(K,\mathbb{Q}(\rho\omega)) \Leftrightarrow$$
$$\sigma(c) = c \text{ για κάθε } c \in \mathbb{Q}(\rho\omega) \Leftrightarrow$$
$$\sigma(\rho\omega) = \rho\omega \Leftrightarrow$$
$$\sigma(\rho)\sigma(\omega) = \rho\omega.$$

Εξετάζοντας όλες τις περιπτώσεις από τον παραπάνω πίνακα, βλέπουμε ότι η τελευταία σχέση αληθεύει αν και μόνο αν $\sigma = \sigma_1, \sigma_6$. Άρα $Gal(K,\mathbb{Q}(\rho\omega)) = \{\sigma_1, \sigma_6\}$.

Το σταθερό σώμα υποομάδας της ομάδας Galois

Έστω επέκταση $F \subseteq K$ και H υποομάδα της $Gal(K,F)$. Θέτουμε

$$FixH = \{a \in K \,|\, \sigma(a) = a \ \ \forall \sigma \in H\}.$$

Είναι σαφές ότι $F \subseteq FixH \subseteq K$ και εύκολα αποδεικνύεται ότι το $FixH$ είναι υπόσωμα του K. Πράγματι, αν $\sigma \in H$ και $a,b \in FixH$, όπου $b \neq 0$, τότε

$$\sigma(a-b) = \sigma(a) - \sigma(b) = a - b \Rightarrow$$
$$a - b \in FixH \text{ και}$$
$$\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1} \Rightarrow$$
$$ab^{-1} \in FixH.$$

Το σώμα $FixH$ λέγεται το **σταθερό σώμα** της υποομάδας H.

Για παράδειγμα, έστω $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ και $H = \{1,\sigma\} \leq Gal(K,\mathbb{Q})$, όπου $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$. (Με το συμβολισμό του Παραδείγματος 4.3 ii), $\sigma = \sigma_2$). Έχουμε $\sqrt{3} \in FixH$. Άρα $\mathbb{Q}(\sqrt{3}) \subseteq FixH$. Επίσης $\sqrt{6} \notin FixH$ αφού

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = -\sqrt{2}\sqrt{3} = -\sqrt{6} \neq \sqrt{6}.$$

Είδαμε πριν ότι αν K είναι πεπερασμένη επέκταση του F, τότε η ομάδα $Gal(K,F)$ είναι πεπερασμένη. Θα δείξουμε τώρα το εξής σημαντικό αποτέλεσμα. Αποτελεί τμήμα του θεμελιώδους θεωρήματος της θεωρίας Galois που θα δούμε στην επόμενη ενότητα.

Προσοχή: Από τώρα και στο εξής, υποθέτουμε ότι κάθε σώμα έχει χαρακτηριστική 0 (εκτός αν αναφέρεται ξεκάθαρα κάτι άλλο). Η υπόθεση αυτή ισχύει για όλα τα αποτελέσματα που ακολουθούν και δεν θα επαναλαμβάνεται στις διατυπώσεις των θεωρημάτων, προτάσεων κλπ.

Θεώρημα 4.4 *Έστω K πεπερασμένη επέκταση του F και H υποομάδα της $Gal(K,F)$. Τότε*

$$|H| = [K : FixH].$$

Ειδικά, $|Gal(K,F)| = [K : FixGal(K,F)]$ που διαιρεί το $[K : F]$.

Απόδειξη Έστω $E = FixH$. Εφαρμόζοντας το Θεώρημα 3.7 στην επέκταση $E \subseteq K$, υπάρχει $a \in K$ με $K = E(a)$. Ξέρουμε ότι η ομάδα H είναι πεπερασμένη αφού είναι υποομάδα της $Gal(K,F)$ που είναι πεπερασμένη (Πρόταση 4.2 iii)). Θεωρούμε τα πολυώνυμο

$$f(x) = \prod_{\sigma \in H} (x - \sigma(a)) \in K[x].$$

Ισχυρισμός: $f(x) = Irr(a,E)$.

Αν αληθεύει ο ισχυρισμός, τότε $|H| = \deg f(x) = \deg Irr(a,E) = [K:E]$ που είναι το ζητούμενο.

Απόδειξη του ισχυρισμού: Παρατηρούμε ότι για κάθε $\tau \in H$,

$$\tau(f(x)) = \prod_{\sigma \in H} (x - \tau\sigma(a)) = \prod_{\sigma \in H} (x - \sigma(a)) = f(x),$$

γιατί καθώς το σ διατρέχει τα στοιχεία της ομάδας H, το ίδιο συμβαίνει για το $\tau\sigma$. Από $\tau(f(x)) = f(x)$ για κάθε $\tau \in H$ έπεται ότι οι συντελεστές του $f(x)$ ανήκουν στο $FixH = E$, δηλαδή

$$f(x) \in E[x].$$

Πράγματι, αν $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$, όπου $a_i \in K$, τότε από $\tau(f(x)) = f(x)$, έχουμε

$$x^n + \tau(a_{n-1})x^{n-1} + ... + \tau(a_0) = x^n + a_{n-1}x^{n-1} + ... + a_0$$

οπότε $\tau(a_i) = a_i$ για κάθε i. Επειδή η τελευταία σχέση ισχύει για κάθε $\tau \in H$, παίρνουμε $a_i \in E$.

Έχουμε $f(x) \in E[x]$ και $f(a) = 0$. Από την Πρόταση 1.3 έπεται ότι στο $E[x]$

$$Irr(a,E) \,|\, f(x).$$

Από τον ορισμό του E, έπεται άμεσα ότι $H \subseteq Gal(K,E)$. Από την Πρόταση 4.2 i) έπεται ότι κάθε $\sigma \in Gal(K,E)$, το $\sigma(a)$ είναι ρίζα του $Irr(a,E)$. Άρα για κάθε $\sigma \in H$, έχουμε $x - \sigma(a) \,|\, Irr(a,E)$ στο $K[x]$. Από την Πρόταση 4.2 ii)) έπεται ότι αν $\sigma, \tau \in Gal(K,E)$ με $\sigma \neq \tau$, τότε $\sigma(a) \neq \tau(a)$. Επομένως

$$f(x) \,|\, Irr(a,E)$$

στο $K[x]$.

Επειδή τα $f(x), Irr(a,E)$ είναι μονικά παίρνουμε $f(x) = Irr(a,E)$.

Η απόδειξη του Θεωρήματος 4.4 παρέχει ένα χρήσιμο τρόπο υπολογισμού ελαχίστων πολυωνύμων. Θα δούμε σχετικό παράδειγμα στο Παράδειγμα 4.8.

Πόρισμα 4.5 *Έστω $F \subseteq F(a)$ πεπερασμένη επέκταση, $H \leq Gal(K,F)$ και $E = FixH$. Τότε*

$$Irr(a,E) = \prod_{\sigma \in H} (x - \sigma(a)).$$

Ομάδα Galois σώματος ριζών

Ξέρουμε ότι αν η επέκταση $F \subseteq K$ είναι πεπερασμένη, τότε $|Gal(K,F)| [K:F]$ (Θεώρημα 4.4). Πότε ισχύει ισότητα;

Θεώρημα 4.6 *Έστω K πεπερασμένη επέκταση του F. Τότε το K είναι σώμα ριζών πάνω από το F αν και μόνο αν $|Gal(K,F)| = [K:F]$.*

Απόδειξη $'\Rightarrow'$ Έστω ότι το K είναι σώμα ριζών πάνω από το F. Από το Πόρισμα 3.10 υπάρχει $a \in K$ τέτοιο ώστε $K = F(a)$ και το K είναι σώμα ριζών του $p(x) = Irr(a,F)$. Το $p(x)$ έχει $n = \deg p(x)$ διακεκριμένες ρίζες $a_1, .., a_n$ (Πρόταση 0.6). Για κάθε $i = 1, ..., n$, έχουμε $Irr(a_i, F) = p(x)$. Άρα για κάθε $i = 1, ..., n$ υπάρχει $\sigma_i \in Gal(K,F)$ με $\sigma_i(a) = a_i$ σύμφωνα με το Πόρισμα 3.11. Συνεπώς

$$|Gal(K,F)| \geq n = \deg Irr(a,K) = [K:F].$$

Από το Θεώρημα 4.4, $|Gal(K,F)| \leq [K:F]$ και άρα $|Gal(K,F)| = [K:F]$.

'$\Leftarrow$' Έστω ότι $|Gal(K,F)| = [K:F]$. Από το Θεώρημα 4.4 έπεται ότι

$$[K:F] = [K:FixGal(K,F)].$$

Επειδή $F \subseteq FixGal(K,F)$ και όλες οι επεκτάσεις είναι πεπερασμένες, παίρνουμε $F = FixGal(K,F)$. Από το Πόρισμα 4.5, το K είναι σώμα ριζών του $Irr(a,F)$, όπου $K = F(a)$ για κάποιο a σύμφωνα με το Θεώρημα 2.6.

Πόρισμα 4.7 *Έστω K πεπερασμένη επέκταση του F. Οι ακόλουθες προτάσεις είναι ισοδύναμες.*

i) Το K είναι σώμα ριζών πάνω από το F.

ii) $F = FixGal(K,F)$.

Απόδειξη Έπεται από το Θεώρημα 4.4 και το Θεώρημα 4.6.

Παράδειγμα 4.8 Έστω $\rho = \sqrt[3]{5}$, $\omega \in \mathbb{C}$ μια ρίζα του πολυωνύμου $x^2 + x + 1$, $K = \mathbb{Q}(\rho,\omega)$ και $a = \rho + \omega$. Θα υπολογίσουμε τα $Irr(a,\mathbb{Q}(\omega\rho))$ και $Irr(a,\mathbb{Q})$.

Στο Παράδειγμα 4.3 ii) προσδιορίσαμε τις ομάδες $Gal(K,\mathbb{Q}) = \{\sigma_1,...,\sigma_6\}$ και $Gal(K,\mathbb{Q}(\omega\rho)) = \{\sigma_1,\sigma_6\}$. Το K είναι σώμα ριζών του $x^3 - 5$ πάνω από το $\mathbb{Q}$. Συνεπώς το K είναι σώμα ριζών πάνω από το $\mathbb{Q}(\rho\omega)$. Από το Πόρισμα 4.7 έπεται ότι

$$FixGal(K,\mathbb{Q}) = \mathbb{Q} \quad \text{και}$$
$$FixGal(K,\mathbb{Q}(\rho\omega)) = \mathbb{Q}(\rho\omega).$$

Από την απόδειξη του Θεωρήματος 3.7 έπεται ότι $K = \mathbb{Q}(a)$. Από το Πόρισμα 4.5

$$Irr(a,\mathbb{Q}(\rho\omega)) = \prod_{\sigma \in Gal(K,\mathbb{Q}(\rho\omega))} (x - \sigma(a)) =$$
$$= (x - \rho - \omega)(x - \rho\omega^2 - \omega^2) =$$
$$= x^2 + (\rho\omega + 1)x + (\rho\omega)^2 - \rho\omega + 1$$

και

$$Irr(a,\mathbb{Q}) = \prod_{\sigma \in Gal(K,\mathbb{Q})} (x - \sigma(a)) =$$
$$= (x - \rho - \omega)(x - \rho - \omega^2)(x - \rho\omega - \omega)(x - \rho\omega - \omega^2)(x - \rho\omega^2 - \omega)(x - \rho\omega^2 - \omega^2) =$$
$$= x^6 + 3x^5 + 6x^4 - 23x^3 - 39x^2 + 48x + 256.$$

Παραδείγματα 4.9

i) Έστω p πρώτος και $K \subseteq \mathbb{C}$ το σώμα ριζών του $x^p - 1$ πάνω από το $\mathbb{Q}$. Τότε $|Gal(K,\mathbb{Q})| = p - 1$.

Πράγματι, έστω $\zeta_p = \cos(2\pi/p) + isin(2\pi/p)$. Ξέρουμε ότι οι ρίζες του $x^p - 1$ είναι οι $1, \zeta_p, \zeta_p^{\,2},..., \zeta_p^{\,p-1}$. Από αυτό έπεται ότι $K = \mathbb{Q}(\zeta_p)$. Στο Παράδειγμα 1.6 iii) είδαμε ότι $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p - 1$, οπότε από το Θεώρημα 4.6 έχουμε $|Gal(K,\mathbb{Q})| = [\mathbb{Q}(\zeta_p):\mathbb{Q}] = p - 1$.

Σημείωση. Η σχέση $|Gal(K,\mathbb{Q})| = p - 1$ μπορεί να αποδειχθεί χωρίς τη χρήση του Θεωρήματος 4.6. Παρατηρούμε ότι αν $\sigma \in Gal(K,\mathbb{Q})$, τότε $\sigma(\zeta_p) \in \{\zeta_p, \zeta_p^{\,2},..., \zeta_p^{\,p-1}\}$ σύμφωνα με την Πρόταση 4.2. Άρα $|Gal(K,\mathbb{Q})| \le p - 1$. Από την άλλη μεριά, για κάθε $a \in \{\zeta_p, \zeta_p^{\,2},..., \zeta_p^{\,p-1}\}$ υπάρχει $\sigma \in Gal(K,\mathbb{Q})$ με $\sigma(\zeta_p) = a$ σύμφωνα με το Πόρισμα 3.11. Άρα $|Gal(K,\mathbb{Q})| \ge p - 1$

ii) Έστω p πρώτος και $K \subseteq \mathbb{C}$ το σώμα ριζών του $x^p - 2$ πάνω από το $\mathbb{Q}$.

a. $K = \mathbb{Q}(a,\zeta_p)$, όπου $a = \sqrt[p]{2} \in \mathbb{R}$.

Πράγματι, οι ρίζες του $x^p - 2$ είναι οι $a\zeta_p^{\,i}, i = 0,..., p-1$. Άρα έχουμε

$K = \mathbb{Q}(a, a\zeta_p, a\zeta_p^{\,2},..., a\zeta_p^{\,p-1}) \subseteq \mathbb{Q}(a,\zeta_p)$. Επειδή $\zeta_p = \dfrac{a\zeta_p}{a} \in K$, ισχύει η ισότητα.

b. $\left|Gal(K,\mathbb{Q})\right| = p(p-1)$.

Έχουμε $Irr(a,\mathbb{Q}) = x^p - 2$ και $Irr(\zeta_p,\mathbb{Q}) = x^{p-1} + x^{p-2} + ... + 1$ (Παραδείγματα 1.4). Επειδή $\mu\kappa\delta(p, p-1) = 1$, από την άσκηση 1.8 παίρνουμε $[\mathbb{Q}(a,\zeta_p):\mathbb{Q}] = p(p-1)$. Επειδή το $K = \mathbb{Q}(a,\zeta_p)$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$, το Θεώρημα 4.6 δίνει $\left|Gal(K,\mathbb{Q})\right| = [K:\mathbb{Q}] = p(p-1)$.

c. Θα περιγράψουμε τα στοιχεία της ομάδας $Gal(K,\mathbb{Q})$.

Επειδή

οι ρίζες του $x^p - 2$ είναι οι $a, a\zeta_p, a\zeta_p{}^2, ..., a\zeta_p{}^{p-1}$

και οι ρίζες του $x^{p-1} + x^{p-2} + ... + 1$ είναι οι $\zeta_p, \zeta_p{}^2, ..., \zeta_p{}^{p-1}$,

συμπεραίνουμε ότι για κάθε $\sigma \in Gal(K,\mathbb{Q})$ ισχύει

$\sigma(a) \in \{a, a\zeta_p, a\zeta_p{}^2, ..., a\zeta_p{}^{p-1}\}$

και $\sigma(\zeta_p) \in \{\zeta_p, \zeta_p{}^2, ..., \zeta_p{}^{p-1}\}$.

Δηλαδή έχουμε το πολύ p δυνατότητες για την τιμή $\sigma(a)$ και το πολύ $p-1$ δυνατότητες για την τιμή $\sigma(\zeta_p)$. Όμως $\left|Gal(K,\mathbb{Q})\right| = p(p-1)$ από το b. Άρα καθεμιά από τις παραπάνω επιλογές δίνει στοιχείο της $Gal(K,\mathbb{Q})$. Δηλαδή,

$$Gal(K,\mathbb{Q}) = \{\sigma_{i,j} \,|\, 0 \le i \le p-1 \text{ και } 1 \le j \le p-1\}, \text{ όπου}$$

$$\sigma_{i,j}(a) = a\zeta_p{}^i \text{ και } \sigma_{i,j}(\zeta_p) = \zeta_p{}^j.$$

d. Η ομάδα $Gal(K,\mathbb{Q})$ δεν είναι αβελιανή αν $p > 2$.

Πάγματι, υπολογίζοντας, για παράδειγμα, τις συνθέσεις $\sigma_{1,0} \circ \sigma_{0,2}$ και $\sigma_{0,2} \circ \sigma_{1,0}$ έχουμε

$$\sigma_{1,0} \circ \sigma_{0,2}(a) = \sigma_{1,0}(a) = a\zeta_p,$$

$$\sigma_{0,2} \circ \sigma_{1,0}(a) = \sigma_{0,2}(a\zeta_p) = \sigma_{0,2}(a)\sigma_{0,2}(\zeta_p) = a\zeta_p{}^2.$$

Άρα $\sigma_{1,0} \circ \sigma_{0,2} \neq \sigma_{0,2} \circ \sigma_{1,0}$.

e. Η ομάδα $Gal(K,\mathbb{Q})$ είναι ισόμορφη με υποομάδα της ομάδας $GL_2(\mathbb{Z}_p)$ των αντιστρέψιμων 2×2 πινάκων με στοιχεία από το $\mathbb{Z}_p$.

Αφήνουμε ως άσκηση την επαλήθευση ότι η απεικόνιση

$$Gal(K,\mathbb{Q}) \to GL_2(\mathbb{Z}_p),\ \sigma_{i,j} \mapsto \begin{pmatrix} [j] & [i] \\ [0] & [1] \end{pmatrix}$$

είναι μονομορφισμός ομάδων, όπου $[m] \in \mathbb{Z}_p$ είναι η κλάση υπολοίπων του m.

iii) Έστω $a = \sqrt{2+\sqrt{2}}$ και $K = \mathbb{Q}(a)$. Θα δείξουμε ότι $\left|Gal(K,\mathbb{Q})\right| = 4$.

Έχουμε $a^2 = 2+\sqrt{2} \Rightarrow (a^2-2)^2 = 2 \Rightarrow a^4 - 4a^2 + 2 = 0$, δηλαδή το a είναι ρίζα του $f(x) = x^4 - 4x^2 + 2$. Το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ σύμφωνα με το κριτήριο του Eisenstein. Άρα $Irr(a,\mathbb{Q}) = f(x)$ και $[K:\mathbb{Q}] = \deg f(x) = 4$.

Παρατηρούμε ότι

$$f(x) = x^4 - 4x^2 + 2 = (x^2 - 2 - \sqrt{2})(x^2 - 2 + \sqrt{2}) =$$

$$(x - \sqrt{2+\sqrt{2}})(x + \sqrt{2+\sqrt{2}})(x - \sqrt{2-\sqrt{2}})(x + \sqrt{2-\sqrt{2}}).$$

Θα δείξουμε ότι κάθε ρίζα του $f(x)$ ανήκει στο K. Έχουμε $a \in K \Rightarrow 2+\sqrt{2} = a^2 \in K \Rightarrow \sqrt{2} \in K$. Από $\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{2}$ έπεται ότι $\sqrt{2-\sqrt{2}} \in K$. Άρα το K είναι σώμα ριζών και επομένως $\left|Gal(K,\mathbb{Q})\right| = [K:\mathbb{Q}] = 4$ σύμφωνα με το Θεώρημα 4.6 (ή σύμφωνα με το Πόρισμα 3.11).

iv) Έστω $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ ανάγωγο, $K \subseteq \mathbb{C}$ το σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$ και $G = Gal(K,\mathbb{Q})$.

a. Ισχύει $|Gal(K,\mathbb{Q})| = 4,8$.

Έστω $d \in \mathbb{C}$ μια λύση της εξίσωσης $x^2 = a^2 - 4b$, $r_1 \in \mathbb{C}$ μια λύση της $x^2 = (-a+d)/2$ και $r_2 \in \mathbb{C}$ μια λύση της $x^2 = (-a-d)/2$. Από

$$x^4 + ax^2 + b = (x^2 - (-a+d)/2)(x^2 - (-a-d)/2) = (x-r_1)(x+r_1)(x-r_2)(x+r_2)$$

παίρνουμε $K = \mathbb{Q}(r_1, r_2)$. Κάθε διαδοχική επέκταση στην ακόλουθη αλυσίδα

$$\begin{array}{c} K = \mathbb{Q}(r_1, r_2) \\ | \\ \mathbb{Q}(r_1) \\ | \\ \mathbb{Q}(d) \\ | \\ \mathbb{Q} \end{array}$$

έχει βαθμό ≤ 2 (γιατί;). Σενεπώς $[K:\mathbb{Q}] = 1,2,4,8$. Επειδή το $f(x) \in \mathbb{Q}[x]$ είναι ανάγωγο βαθμού 4, παίρνουμε $4 = [\mathbb{Q}(r_1):\mathbb{Q}] \leq [K:\mathbb{Q}]$, οπότε $[K:\mathbb{Q}] = 4,8$. Επειδή το K είναι σώμα ριζών πάνω από το $\mathbb{Q}$, έχουμε $|Gal(K,\mathbb{Q})| = [K:\mathbb{Q}] = 4,8$ σύμφωνα με το Θεώρημα 4.6.

b. Έστω ότι το b είναι τετράγωνο ρητού . Θα δείξουμε ότι $Gal(K,\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Έχουμε τη σχέση $r_1^2 r_2^2 = b$. Τότε $r_1 r_2 = c \in \mathbb{Q}$ και άρα $K = \mathbb{Q}(r_1)$. Συνεπώς $[K:\mathbb{Q}] = 4$ και $|Gal(K,\mathbb{Q})| = 4$. Θα δείξουμε τώρα ότι $\sigma^2 = 1_K$ για κάθε $\sigma \in Gal(K,\mathbb{Q})$. Πράγματι, έχουμε $\sigma(r_1) \in \{r_1, -r_1, r_2, -r_2\}$. Αν $\sigma(r_1) = \pm r_1$, το ζητούμενο είναι σαφές. Αν $\sigma(r_1) = \pm r_2$, τότε $\sigma^2(r_1) = \pm\sigma(r_2) = \pm\sigma(cr_1^{-1}) = \pm c\sigma(r_1)^{-1} = r_1$. Επειδή $|Gal(K,\mathbb{Q})| = 4$ και η ομάδα δεν έχει στοιχείο τάξης 4, έπεται ότι είναι ισόμορφη με τη $\mathbb{Z}_2 \times \mathbb{Z}_2$.

c. Έστω ότι το $b(a^2 - 4b)$ είναι τετράγωνο ρητού. Θα δείξουμε ότι $Gal(K,\mathbb{Q}) \simeq \mathbb{Z}_4$.

Με το συμβολισμό του μέρους a έχουμε τις σχέσεις $r_1^2 - r_2^2 = d$ και $r_1^2 r_2^2 = b$. Παρατηρούμε ότι επειδή το $f(x) \in \mathbb{Q}[x]$ είναι ανάγωγο έχουμε $d \neq 0$. Από την υπόθεση έχουμε $r_1 r_2 d \in \mathbb{Q}$. Από τις σχέσεις $r_1^2 = \dfrac{-a+d}{2}$ και $r_1 r_2 d \in \mathbb{Q}$ έπεται ότι $r_2 \in \mathbb{Q}(r_1)$ και επομένως $K = \mathbb{Q}(r_1)$.

Τοτε $[K:\mathbb{Q}] = 4$ και άρα $|Gal(K,\mathbb{Q})| = 4$. Θα δείξουμε τώρα ότι η ομάδα $Gal(K,\mathbb{Q})$ περιέχει στοιχείο τάξης 4. Από το Πόρισμα 3.11 έπεται ότι υπάρχει $\sigma \in Gal(K,\mathbb{Q})$ με $\sigma(r_1) = r_2$. Έστω, για άτοπο, ότι $\sigma^2 = 1_K$, οπότε $\sigma(r_2) = r_1$. Από $r_1^2 - r_2^2 = d$ παίρνουμε $\sigma(d) = -d$, που λόγω της $r_1 r_2 d \in \mathbb{Q}$ δίνει $\sigma(d) = 0$, δηλαδή $d = 0$, άτοπο.

Μεταθέσεις ριζών

Έστω K ένα σώμα ριζών του $f(x) \in F[x]$ πάνω από το F, οπότε $f(x) = c(x-a_1)(x-a_2)...(x-a_n)$, όπου $c, a_i \in K$. Ξέρουμε ότι κάθε $\sigma \in Gal(K,F)$ απεικονίζει τις ρίζες της $f(x)$ στις ρίζες της $f(x)$ (Πρόταση 4. 2 i)). Αν υποθέσουμε ότι οι $a_1,....,a_n$ είναι ανά δύο διαφορετικές, τότε ο περιορισμός της απεικόνισης σ στο πεπερασμένο σύνολο $\{a_1,...,a_n\}$ ορίζει μια απεικόνιση $\bar{\sigma}: \{a_1,...,a_n\} \to \{a_1,...,a_n\}$, που είναι 1-1 και άρα επί. **Δηλαδή η $\bar{\sigma}$ είναι μια μετάθεση του συνόλου $\{a_1,...,a_n\}$.** Εύκολα επαληθεύεται ότι η αντιστοιχία $Gal(K,F) \to S_X, \sigma \mapsto \bar{\sigma}$, είναι μονομορφισμός ομάδων, όπου $X = \{a_1,...,a_n\}$ και S_X είναι η ομάδα μεταθέσεων του X.

Παράδειγμα Έστω $\rho = \sqrt[3]{5}$, $\omega = (-1+i\sqrt{3})/2$ και $K = \mathbb{Q}(\rho, \omega)$. Το K είναι σώμα ριζών του $x^3 - 5$ πάνω από το $\mathbb{Q}$. Στο Παράδειγμα 1.11 (ή πιο πρόσφατα, στο Παράδειγμα 4.9 ii) με $\sqrt[3]{2}$ στη θέση του $\sqrt[3]{5}$) είδαμε ότι υπάρχει ισομορφισμός $\sigma : K \to K$ με

$$\sigma(\rho) = \rho\omega^2,$$
$$\sigma(\omega) = \omega^2.$$

Από τις σχέσεις αυτές εύκολα υπολογίζουμε ότι

$$\sigma(\rho\omega) = \sigma(\rho)\sigma(\omega) = \rho\omega^2\omega^2 = \rho\omega$$
$$\sigma(\rho\omega^2) = \sigma(\rho)\sigma(\omega)^2 = \rho\omega^2\omega^4 = \rho.$$

Συνεπώς η απεικόνιση σ δίνει τη μετάθεση

$$\bar{\sigma} = \begin{pmatrix} \rho & \rho\omega & \rho\omega^2 \\ \rho\omega^2 & \rho\omega & \rho \end{pmatrix}$$

του συνόλου $\{\rho, \rho\omega, \rho\omega^2\}$. Κάτω από την αντιστοίχιση $\rho \leftrightarrow 1, \rho\omega \leftrightarrow 2, \rho\omega^2 \leftrightarrow 3$, η μετάθεση $\bar{\sigma}$ αντιστοιχεί στο στοιχείο $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ της συμμετρικής ομάδας S_3.

Πρόταση 4.10 *Έστω $f(x) \in F[x]$ και K σώμα ριζών του $f(x)$ πάνω από το F. Τότε η ομάδα $Gal(K, F)$ είναι ισόμορφη με υποομάδα της συμμετρικής ομάδας S_n, όπου $n =$ πλήθος των διακεκριμένων ριζών του $f(x)$ στο K. Ειδικά, αν το $f(x)$ είναι ανάγωγο πάνω από το F, τότε $n = \deg f(x)$.*

Απόδειξη Το ότι η $Gal(K, F)$ είναι ισόμορφη με υποομάδα της συμμετρικής ομάδας S_n έπεται από αυτά που αναφέραμε πιο πάνω. Το τελευταίο συμπέρασμα της πρότασης έπεται το ότι κάθε ανάγωγο $p(x) \in F[x]$ δεν έχει πολλαπλές ρίζες σε επέκταση του F (Πρόταση 0.8).

Ξέρουμε ότι η ομάδα Galois σώματος ριζών K πολυωνύμου $f(x) \in F[x]$ μεταθέτει τις ρίζες του $f(x)$. Ποιες μεταθέσεις προκύπτουν με τον τρόπο αυτό; Ήδη η Πρόταση 4.2 i) (βλ. και Πόρισμα 3.11) θέτει έναν περιορισμό: *Αν $a \in K$ είναι ρίζα ενός ανάγωγου παράγοντα του $f(x)$ πάνω από το F, τότε για κάθε $\sigma \in Gal(K, F)$, το $\sigma(a)$ είναι ρίζα του ίδιου ανάγωγου παράγοντα.* Όμως υπάρχουν και άλλοι περιορισμοί, που ίσως είναι λιγότερο εμφανείς, όπως δείχνει το δεύτερο από τα επόμενα παραδείγματα.

Παραδείγματα 4.11

i) Θα δείξουμε ότι $Gal(K, \mathbb{Q}) \simeq S_3$, όπου $K \subseteq \mathbb{C}$ είναι το σώμα ριζών του $p(x) = x^3 + 3x + 1$ πάνω από το $\mathbb{Q}$.

Το $p(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ καθώς δεν έχει ρητή ρίζα (Πρόταση 0.1) και είναι τρίτου βαθμού. Το πολυώνυμο $p(x)$ έχει μοναδική πραγματική ρίζα. Πράγματι, είναι περιττού βαθμού και έχει πραγματικούς συντελεστές. Άρα έχει πραγματική ρίζα, έστω a. Η παράγωγος του $p(x)$ είναι $3x^2 + 3$ που είναι θετική για κάθε $x \in \mathbb{R}$. Συνεπώς η συνάρτηση $\mathbb{R} \to \mathbb{R},\ x \mapsto x^3 + 3x + 1,$ είναι γνήσια αύξουσα. Άρα υπάρχει μοναδική πραγματική ρίζα του $p(x)$.

Αν $b \in \mathbb{C}$ είναι ρίζα του $p(x)$ διάφορη της a, τότε $b \notin \mathbb{R}$. Συνεπώς $b \notin \mathbb{Q}(a)$ και $[\mathbb{Q}(a,b) : \mathbb{Q}] > [\mathbb{Q}(a) : \mathbb{Q}] = 3$. Άρα $[K : \mathbb{Q}] > 3$, οπότε από το Θεώρημα 4.4 έχουμε

$$\left|Gal(K, \mathbb{Q})\right| = [K : \mathbb{Q}] > 3.$$

Από την Πρόταση 4.10 έπεται ότι $Gal(K, \mathbb{Q}) \simeq S_3$.

ii) Θα δείξουμε ότι $Gal(K, \mathbb{Q}) \neq S_3$, όπου $K \subseteq \mathbb{C}$ είναι το σώμα ριζών του $p(x) = x^3 - 3x + 1$ πάνω από το $\mathbb{Q}$.

Για το σκοπό αυτό θα χρησιμοποιήσουμε το ακόλουθο αποτέλεσμα. Έστω $a,b,c \in \mathbb{C}$ οι ρίζες του πολυωνύμου $x^3 + px + q$ και $\Delta = (a-b)(a-c)(b-c)$. Τότε $\Delta^2 = -4p^3 - 27q^2$. [1]
Επειδή το $p(x)$ δεν έχει ρητή ρίζα και είναι τρίτου βαθμού, συμπεραίνουμε ότι το $p(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$. Σύμφωνα με την Πρόταση 4.10, η ομάδα $Gal(K,\mathbb{Q})$ είναι ισόμορφη με υποομάδα της S_3. Θα δείξουμε ότι δεν υπάρχει $\sigma \in Gal(K,\mathbb{Q})$ τέτοιο ώστε

$$\sigma(a) = b,$$
$$\sigma(b) = a,$$
$$\sigma(c) = c,$$

όπου $a,b,c \in K$ είναι οι ρίζες του $f(x)$. Με άλλα λόγια, η μετάθεση $\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$ δεν προκύπτει από τη δράση της $\sigma \in Gal(K,\mathbb{Q})$ στο σύνολο $\{a,b,c\}$.

Για άτοπο, έστω ότι υπάρχει $\sigma \in Gal(K,\mathbb{Q})$ με $\sigma(a) = b, \sigma(b) = a, \sigma(c) = c.$ Θεωρούμε το στοιχείο $\Delta = (a-b)(a-c)(b-c)$. Παρατηρούμε ότι

$$\sigma(\Delta) = (\sigma(a) - \sigma(b))(\sigma(a) - \sigma(c))(\sigma(b) - \sigma(c)) = (b-a)(b-c)(a-b),$$

δηλαδή

$$\sigma(\Delta) = -\Delta.$$

Όμως, από τη σχέση $\Delta^2 = -4p^3 - 27q^2$ που αναφέραμε πριν, έχουμε $\Delta^2 = 81$. Άρα $\Delta = 9$ ή $\Delta = -9$. Σε κάθε περίπτωση, $\Delta \in \mathbb{Q}$. Άρα $\sigma(\Delta) = \Delta$ αφού $\sigma \in Gal(K,\mathbb{Q})$, άτοπο.

Σχόλιο. Από την Πρόταση 4.10 η τάξη $|Gal(K,\mathbb{Q})|$ διαιρεί το 6. Δείξαμε στο παράδειγμα ότι $|Gal(K,\mathbb{Q})| < 6$. Από το Θεώρημα 4.6 έχουμε $|Gal(K,\mathbb{Q})| = [K:\mathbb{Q}] \geq [\mathbb{Q}(a):\mathbb{Q}] = 3$. Άρα $[K:\mathbb{Q}] = 3$, οπότε $K = \mathbb{Q}(a)$. Αυτό σημαίνει ότι $b,c \in \mathbb{Q}(a)$, δηλαδή

$$\textit{τα } b,c \textit{ είναι } \mathbb{Q} \textit{ - γραμμικοί συνδυασμοί των } 1,a,a^2.$$

Αυτή η 'αλληλοεξάρτηση' των ριζών είναι ο ουσιαστικός λόγος που $|Gal(K,\mathbb{Q})| < 6$.

Ασκήσεις 4

1. Βρείτε την ομάδα $Gal(K,F)$ στις ακόλουθες περιπτώσεις και εξετάστε αν είναι κυκλική.
   a. $F = \mathbb{Q}, \quad K = \mathbb{Q}(i,\sqrt{2})$.
   b. $F = \mathbb{Q}(i), \quad K = \mathbb{Q}(i,\sqrt{2})$.
   c. $F = \mathbb{Q}(\sqrt{2}), \quad K = \mathbb{Q}(\sqrt[4]{2})$.
   d. $F = \mathbb{Q}, \quad K = \mathbb{Q}(\sqrt[4]{2})$.
   e. $F = \mathbb{Q}, \quad K = \mathbb{Q}(a)$ όπου $a \in \mathbb{C}$ ρίζα του $x^2 + x + 2$.
2. Ποια είναι η ομάδα Galois σώματος ριζών του $x^3 - x^2 - 4$ πάνω από το $\mathbb{Q}$;
3. Έστω $K \subseteq \mathbb{C}$ σώμα ριζών πάνω από το $\mathbb{Q}$ που δεν περιέχεται στο $\mathbb{R}$. Τότε η τάξη $|Gal(K,\mathbb{Q})|$ είναι άρτιος ακέραιος.
4. Ποια είναι η ομάδα Galois σώματος ριζών του $x^3 + x - 1$ πάνω από το $\mathbb{Q}$;
5. Χρησιμοποιείστε το Πόρισμα 4.5 για να υπολογίσετε το $Irr(\sqrt{2} - 2\sqrt{3}, \mathbb{Q})$.
6. Αποδείξτε τον τελευταίο ισχυρισμό στο Παράδειγμα 4.9 ii).
7. Δείξτε ότι η ομάδα Galois της επέκτασης
   a. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2+\sqrt{2}})$ έχει τάξη 4 και είναι κυκλική (βλ. Παράδειγμα 4.9 ii),
   b. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2+\sqrt{3}})$ έχει τάξη 4 και δεν είναι κυκλική.

[1] Το Δ^2 ονομάζεται η διακρίνουσα του $x^3 + px + q$. Περισσότερα για το Δ^2 θα δούμε στην επόμενη ενότητα.

8. Έστω $f(x) \in \mathbb{Q}[x]$ βαθμού 3 και K σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$. Αν υπάρχει $\sigma \in Gal(K, \mathbb{Q})$ τάξης 3, τότε το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$.
9. Έστω $f(x) = x^3 + ax + b \in \mathbb{Q}[x]$ ανάγωγο πάνω από το $\mathbb{Q}$ και $K \subseteq \mathbb{C}$ σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$. Δείξτε ότι οι ακόλουθες προτάσεις είναι ισοδύναμες.
    a. $\left|Gal(K:\mathbb{Q})\right| \neq 6$.
    b. $\left|Gal(K:\mathbb{Q})\right| = 3$.
    c. Υπάρχουν ρίζες $r, s \in \mathbb{C}$ του $f(x)$, τέτοιες ώστε $s = \lambda + \mu r + \nu r^2$ για κάποια $\lambda, \mu, \nu \in \mathbb{Q}$.
10. Δείξτε ότι
    a. η ομάδα $Gal(\mathbb{R}, \mathbb{Q})$ είναι τετριμμένη και
    b. η ομάδα $Gal(\mathbb{Q}(\pi), \mathbb{Q})$ είναι άπειρη. (Θεωρούμε γνωστό ότι το π δεν είναι αλγεβρικό πάνω από το $\mathbb{Q}$).
11. Έστω $f(x) = x^3 + x^2 - 2x - 1$ και $a \in \mathbb{C}$ μια ρίζα του. Δείξτε τα εξής.
    a. Το $a^2 - 2$ είναι ρίζα του $f(x)$.
    b. Το σώμα ριζών του $f(x)$ στο $\mathbb{C}$ πάνω από το $\mathbb{Q}$ είναι το $\mathbb{Q}(a)$.
    c. Υπάρχει $\sigma \in Gal(\mathbb{Q}(a), \mathbb{Q})$ με $\sigma(a) = a^2 - 2$. Επίσης $\left|Gal(K:\mathbb{Q})\right| = 3$.
12. Έστω $a \in \mathbb{C}$ και $K = \mathbb{Q}(a)$, όπου $a^2 = \dfrac{3 + i\sqrt{7}}{2}$ και $K = \mathbb{Q}(a)$.
    a. Υπολογίστε το βαθμό $[K:\mathbb{Q}]$.
    b. Βρείτε τα $Irr(a, \mathbb{Q})$, $Irr(a, \mathbb{Q}(a^2))$, $Irr(a^2, \mathbb{Q})$.
    c. Αληθεύει ότι το K είναι σώμα ριζών πάνω από το $\mathbb{Q}$;
    d. Δείξτε ότι η ομάδα $Gal(K, \mathbb{Q})$ δεν είναι κυκλική και βρείτε όλες τις υποομάδες της.
    e. Αληθεύει ότι $\sqrt{7} \in K$;
13. Έστω $f(x) \in \mathbb{Q}[x]$ τέτοιο ώστε μκδ$(f(x), f'(x)) = 1$. Τότε το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ αν και μόνο αν για κάθε δύο ρίζες $a, b \in \mathbb{C}$ του $f(x)$ υπάρχει $\sigma \in Gal(K, \mathbb{Q})$ με $\sigma(a) = b$, όπου $K \subseteq \mathbb{C}$ είναι το σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$.
14. Έστω p πρώτος. Δείξτε ότι η ομάδα Galois του σώματος ριζών του $x^4 - p$ στο $\mathbb{C}$ πάνω από το $\mathbb{Q}$ έχει τάξη 8.
15. Έστω $f(x) \in \mathbb{Q}[x]$ βαθμού $n > 2$, $K \subseteq \mathbb{C}$ σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$ και $G = Gal(K, \mathbb{Q})$. Υποθέτουμε ότι $G \simeq S_n$. Δείξτε τα εξής.
    a. Το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$.
    b. Αν το $a \in K$ είναι ρίζα του $f(x)$, τότε $Gal(\mathbb{Q}(a), \mathbb{Q}) = 1$.
16. Εξετάστε ποιες από τις επόμενες προτάσεις αληθεύουν.
    a. Υπάρχουν διαδοχικές πεπερασμένες επεκτάσεις $F \subseteq E \subseteq K$ με $Gal(K, F) \simeq \mathbb{Z}_3$ και $Gal(K, E) \simeq \mathbb{Z}_2$.
    b. Αν $F \subseteq K_1$ και $F \subseteq K_2$ είναι επεκτάσεις τέτοιε ώστε οι ομάδες $Gal(K_1, F), Gal(K_2, F)$ είναι ισόμορφες, τότε τα σώματα K_1, K_2 είναι ισόμορφα.
    c. Υπάρχει $f(x) \in \mathbb{Q}[x]$ βαθμού 4 τέτοιο ώστε $\left|Gal(K, \mathbb{Q})\right| = 16$, όπου K σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$.

5. Το Θεμελιώδες Θεώρημα της Θεωρίας Galois

Βασικά σημεία

- Το θεμελιώδες θεώρημα.
- Παραδείγματα αντιστοιχίας Galois.
- Η ομάδα Galois τριτοβάθμιου πολυωνύμου.

Στην ενότητα αυτή υποθέτουμε ότι *κάθε σώμα έχει χαρακτηριστική 0.* Επίσης, το K είναι *πεπερασμένη* επέκταση του F.

Αντιστοιχία Galois

Ξέρουμε ότι αν E είναι σώμα με $F \subseteq E \subseteq K$, τότε η ομάδα $Gal(K,E)$ είναι υποομάδα της $Gal(K,F)$. Επομένως έχουμε μια απεικόνιση

$$Gal(K,-): \mathcal{F} \to \mathcal{G},\ E \mapsto Gal(K,E)$$

όπου $\mathcal{F}$ είναι το σύνολο των σωμάτων E με $F \subseteq E \subseteq K$ και $\mathcal{G}$ είναι το σύνολο των υποομάδων της $Gal(K,F)$.

Στην προηγούμενη ενότητα είδαμε ότι αν $H \leq Gal(K,F)$, τότε το σταθερό σώμα

$$FixH = \{a \in K \,|\, \sigma(a) = a \ \ \forall \sigma \in H\}$$

είναι ένα υπόσωμα του K με $F \subseteq FixH \subseteq K$. Συνεπώς έχουμε την απεικόνιση

$$Fix(-): \mathcal{G} \to \mathcal{F},\ H \mapsto FixH\,.$$

Οι παραπάνω απεικονίσεις παρίστανται στα ακόλουθα διαγράμματα.

$$\begin{array}{ccc} K & & 1 \\ | & & | \\ E & \xrightarrow{E \mapsto Gal(K,E)} & Gal(K,E) \\ | & & | \\ F & & Gal(K,F) \end{array} \qquad\qquad \begin{array}{ccc} 1 & & K \\ | & & | \\ H & \xrightarrow{H \mapsto FixH} & FixH \\ | & & | \\ Gal(K,F) & & F \end{array}$$

Με 1 συμβολίζουμε την τετριμμένη ομάδα. Η εικόνα του K μέσω της απεικόνισης $Gal(K,-): \mathcal{F} \to \mathcal{G}$ είναι η ομάδα $Gal(K,K) = 1$. Τα διαγράμματα των υποομάδων είναι 'ανεστραμμένα'.

Παρατηρήσεις 5.1

i) Έστω $E_1, E_2 \in \mathcal{F}$ με $E_1 \subseteq E_2$ και έστω $H_1, H_2 \in \mathcal{G}$ με $H_1 \subseteq H_2$. Από τους ορισμούς έπεται άμεσα ότι $Gal(K,E_1) \supseteq Gal(K,E_2)$ και $FixH_1 \supseteq FixH_2$. Δηλαδή οι απεικονίσεις $Gal(K,-)$ και $Fix(-)$ αναστρέφουν τη σχέση υποσυνόλου.

ii) Σημειώνουμε ότι το Πόρισμα 4.7 λέει ότι το K είναι σώμα ριζών πάνω από το F αν και μόνο αν $F = FixGal(K,F)$.

Παράδειγμα 5.2

Έστω $\rho = \sqrt[3]{5}$, $\omega \in \mathbb{C}$ μια ρίζα του πολυωνύμου $x^2 + x + 1$ και $K = \mathbb{Q}(\rho, \omega)$. Με το συμβολισμό του Παραδείγματος 4.3 iii), έστω $H = \{\sigma_1, \sigma_6\} \leq Gal(K,\mathbb{Q})$, όπου $\sigma_6(\rho) = \rho\omega^2$, $\sigma_6(\omega) = \omega^2$. Θα προσδιορίσουμε το σώμα $FixH$.

Έστω $\sigma = \sigma_6$. Μια βάση του $K = \mathbb{Q}(\rho,\omega)$ ως $\mathbb{Q}$- διανυσματικός χώρος είναι το σύνολο $\{1, \rho, \rho^2, \omega, \omega\rho, \omega\rho^2\}$ όπως είδαμε στο Παράδειγμα 1.8 ii). Έστω $a \in K$, οπότε $a = c_0 + c_1\rho + c_2\rho^2 + c_3\omega + c_4\omega\rho + c_5\omega\rho^2$, όπου $c_i \in \mathbb{Q}$. Τότε

$$\begin{aligned}\sigma(a) &= c_0 + c_1\sigma(\rho) + c_2\sigma(\rho)^2 + c_3\sigma(\omega) + c_4\sigma(\omega)\sigma(\rho) + c_5\sigma(\omega)\sigma(\rho)^2 = \\ &= c_0 + c_1\omega^2\rho + c_2\omega^4\rho^2 + c_3\omega^2 + c_4\omega^4\rho + c_5\omega^6\rho^2 = \\ &= c_0 + c_1\omega^2\rho + c_2\omega\rho^2 + c_3\omega^2 + c_4\omega\rho + c_5\rho^2 = \\ &= c_0 + c_1(-\omega-1)\rho + c_2\omega\rho^2 + c_3(-1-\omega) + c_4\omega\rho + c_5\rho^2 = \\ &= c_0 - c_3 + (-c_1)\rho + c_5\rho^2 + (-c_3)\omega + (-c_1 + c_4)\omega\rho + c_2\omega\rho^2.\end{aligned}$$

Άρα έχουμε

$$a \in FixH \Leftrightarrow a = \sigma(a) \Leftrightarrow \begin{cases} c_0 = c_0 - c_3 \\ c_1 = -c_1 \\ c_2 = c_5 \\ c_3 = -c_3 \\ c_4 = -c_1 + c_4 \\ c_5 = c_2 \end{cases} \Leftrightarrow \begin{cases} c_1 = 0 \\ c_3 = 0 \\ c_2 = c_5 \end{cases} \Leftrightarrow a = c_0 + c_2\rho^2 + c_4\omega\rho + c_2\omega\rho^2.$$

Παρατηρούμε ότι

$$c_0 + c_2\rho^2 + c_4\omega\rho + c_2\omega\rho^2 = c_0 + c_4\omega\rho + c_2(1+\omega)\rho^2 = c_0 + c_4\omega\rho - c_2(\omega\rho)^2.$$

Συνεπώς $FixH = \mathbb{Q}(\omega\rho)$.[1]

Το κύριο αποτέλεσμα του μαθήματος είναι το ακόλουθο.

Θεώρημα 5.3 (θεμελιώδες θεώρημα θεωρίας Galois) *Έστω K σώμα ριζών πάνω από το F και $G = Gal(K,F)$. Έστω $E \in \mathcal{F}$ και $H \in \mathcal{G}$. Ισχύουν οι ακόλουθες προτάσεις.*

i) $Fix(Gal(K,E)) = E$ *και* $Gal(K,FixH) = H$.
Δηλαδή, η απεικόνιση $Gal(K,-): \mathcal{F} \to \mathcal{G}$ είναι 1-1 και επί και η αντίστροφή της είναι η απεικόνιση $Fix(-): \mathcal{G} \to \mathcal{F}$.

ii) $[E:F] = [G:Gal(E,F)]$ *και* $[G:H] = [FixH:F]$.

iii) Το E είναι σώμα ριζών πάνω από το F αν και μόνο αν η $Gal(K,E)$ είναι κανονική υποομάδα της G. Στην περίπτωση αυτή υπάρχει ισομορφισμός ομάδων $G/Gal(K,E) \simeq Gal(E,F)$.

$$\begin{array}{ccc} K & & 1 \\ | & & | \\ E & \xrightarrow{E \mapsto Gal(K,E)} & Gal(K,E) \\ | \ \}[E:F] & & | \ \}[G:Gal(K,E)] \\ F & & G \end{array} \qquad \begin{array}{ccc} 1 & & K \\ | & & | \\ H & \xrightarrow{H \mapsto FixH} & FixH \\ | \ \} \ [G:H] & & | \ \} \ [FixH:F] \\ G & & F \end{array}$$

Απόδειξη i) Από την Παρατήρηση 3.3, το K είναι σώμα ριζών πάνω από το E. Από το Πόρισμα 4.7 έχουμε $Fix(Gal(K,E)) = E$.

Από τους ορισμούς έπεται άμεσα ότι $Gal(K,FixH) \supseteq H$. Από το Θεώρημα 4.4 έχουμε

$$|H| = [K:FixH].$$

Από το ίδιο θεώρημα έχουμε (για $FixH$ στη θέση του F)

$$|Gal(K,FixH)| \le [K:FixH]$$

και επομένως $|Gal(K,FixH)| \le |H|$. Συνεπώς $Gal(K,FixH) = H$ γιατί οι ομάδες αυτές είναι πεπερασμένες.

[1] Αν ξέραμε ότι $H = Gal(K,\mathbb{Q}(\omega\rho))$, τότε από το Πόρισμα 4.7 θα είχαμε $FixH = \mathbb{Q}(\omega\rho)$, γιατί το K είναι σώμα ριζών πάνω από το $\mathbb{Q}(\omega\rho)$. Το παράδειγμα δείχνει έναν τρόπο υπολογισμού του $FixH$ χωρίς a priori γνώση της απάντησης ή υποψήφιας απάντησης. Φυσικά ο υπολογισμός στο παράδειγμα δεν απαιτεί το K να είναι σώμα ριζών.

ii) Από το Θεώρημα 1.10, το Θεώρημα 4.6, την Παρατήρηση 3.3 και το θεώρημα του Lagrange για ομάδες έχουμε διαδοχικά

$$[E:F]=[K:F]/[K:E]=|G|/|Gal(K,E)|=[G:Gal(K,E)].$$

Από το i) έχουμε $|H|=|Gal(K,FixH)|$ και άρα

$$[G:H]=|G|/|H|=|G|/|Gal(K,FixH)|=[K:F]/[K:FixH]=[FixH:F]$$

iii) Η υποομάδα $Gal(K,E)$ είναι κανονική στη G αν και μόνο αν $\sigma(a)\in E\ \ \forall\sigma\in G,\forall a\in E$. Πράγματι,

$$\sigma^{-1}h\sigma\in Gal(K,E)\ \ \forall\sigma\in G,\forall h\in Gal(K,E)\Leftrightarrow$$
$$\sigma^{-1}h\sigma(a)=a\ \ \forall\sigma\in G,\forall h\in Gal(K,E),\forall a\in E\Leftrightarrow$$
$$h(\sigma(a))=\sigma(a)\ \ \forall\sigma\in G,\forall h\in Gal(K,E),\forall a\in E\Leftrightarrow$$
$$\sigma(a)\in Fix(Gal(K,E))\ \ \forall\sigma\in G,\forall a\in E\Leftrightarrow$$
$$\sigma(a)\in E\ \ \forall\sigma\in G,\forall a\in E,$$

όπου στην τελευταία ισοδυναμία χρησιμοποιήσαμε το i) του θεωρήματος.

Η συνθήκη $\sigma(a)\in E\ \ \forall\sigma\in G,\forall a\in E$ σημαίνει ότι για κάθε $\sigma\in G$, ο περιορισμός σ_E της απεικόνισης σ στο E είναι απεικόνιση $\sigma_E:E\to E$. Μάλιστα, $\sigma_E\in Gal(E,F)$ καθώς η σ_E είναι μονομορφισμός και άρα $\dim\mathrm{Im}\,\sigma_E=\dim E$ που είναι πεπερασμένη, οπότε η σ_E είναι επί.

$'\Rightarrow'$ Έστω ότι το E είναι σώμα ριζών πάνω από το F. Από το Λήμμα 3.8 έπεται ότι $\sigma(a)\in E\ \ \forall\sigma\in G,\forall a\in E$. Άρα η $Gal(K,E)$ είναι κανονική στη G.

$'\Leftarrow'$ Έστω ότι η $Gal(K,E)$ είναι κανονική στη G, δηλαδή $\sigma(a)\in E\ \ \forall\sigma\in G,\forall a\in E$. Ισχυριζόμαστε ότι

$$\{c\in E\,|\,h(c)=c\ \ \forall h\in Gal(E,F)\}=F.$$

Πράγματι, αν c ανήκει στο αριστερό μέλος, τότε $\sigma_E(c)=c\ \ \forall\sigma\in G$, δηλαδή $\sigma(c)=c\ \ \forall\sigma\in G$. Άρα $c\in FixG=F$ σύμφωνα με το Πόρισμα 4.7. Δηλαδή $\{c\in E\,|\,h(c)=c\ \ \forall h\in Gal(E,F)\}\subseteq F$. Η άλλη σχέση $\{c\in E\,|\,h(c)=c\ \ \forall h\in Gal(E,F)\}\supseteq F$ είναι σαφής και άρα έχουμε ισότητα. Από το Πόρισμα 4.7 έπεται ότι το E είναι σώμα ριζών πάνω από το F.

Έστω ότι το E είναι σώμα ριζών πάνω από το F. Θεωρούμε την απεικόνιση

$$\varphi:G\to Gal(E,F),\ \varphi(\sigma)=\sigma_E,$$

όπου σ_E είναι ο περιορισμός της απεικόνισης σ στο E. Είδαμε πριν ότι πράγματι $\sigma_E\in Gal(E,F)$. Είναι σαφές ότι η φ είναι ομομορφισμός ομάδων και $\ker\varphi=Gal(K,E)$. Από το πρώτο θεώρημα ισομορφισμών ομάδων έχουμε $G/Gal(K,E)\simeq\mathrm{Im}\,\varphi$. Μένει να δείξουμε ότι η φ είναι επί.

Έστω $\tau\in Gal(E,F)$. Από το Λήμμα 3.5 υπάρχει $\sigma\in G$ που επεκτείνει τον τ. Άρα $\tau=\sigma_E$ και η φ είναι επί.

Παρατήρηση 5.4 Στην απόδειξη του i) του προηγούμενου θεωρήματος της σχέσης

$$Gal(K,FixH)=H,$$

δεν χρησιμοποιήσαμε την υπόθεση ότι το K είναι σώμα ριζών πάνω από το F παρά μόνο ότι είναι πεπερασμένη επέκταση. Συνεπώς η σχέση αυτή ισχύει για κάθε πεπερασμένη επέκταση K του F.

Ακολουθούν μερικά παραδείγματα της αντιστοιχίας Galois. Το Παράδειγμα 5.7 είναι το πιο ενδεικτικό.

Παράδειγμα 5.5 Έστω $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ και $G=Gal(K,\mathbb{Q})$. Το K είναι σώμα ριζών του $(x^2-2)(x^2-3)$ πάνω το $\mathbb{Q}$. Στο Παράδειγμα 4.3 ii) υπολογίσαμε ότι $G=\{1,\sigma_2,\sigma_3,\sigma_4\}$ όπου τα σ_i ορίζονται από τον παρακάτω πίνακα.

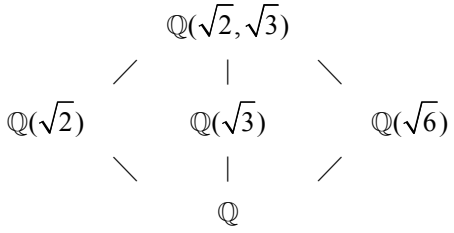
G	$\sigma_i(\sqrt{2}) = \ldots$	$\sigma_i(\sqrt{3}) = \ldots$
$\sigma_1 = 1$	$\sqrt{2}$	$\sqrt{3}$
σ_2	$\sqrt{2}$	$-\sqrt{3}$
σ_3	$-\sqrt{2}$	$\sqrt{3}$
σ_4	$-\sqrt{2}$	$-\sqrt{3}$

Οι υποομάδες της G είναι οι

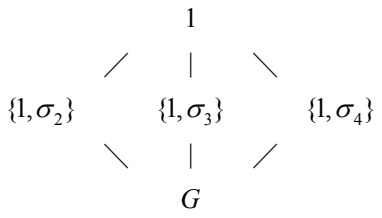
$$1, \{1, \sigma_2\}, \{1, \sigma_3\}, \{1, \sigma_4\}, G .$$

Το διάγραμμα των υποομάδων της G δίνεται παρακάτω. Για κάθε υποομάδα H της G υπολογίζουμε το $FixH$ και έτσι προκύπτει το διάγραμμα των υποσωμάτων του $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, σύμφωνα με το Θεώρημα 5.3. Εννοούμε ότι σε αντίστοιχες θέσεις των δύο διαγραμμάτων υπάρχουν αντίστοιχα αντικείμενα. Για παράδειγμα, $Gal(K, \mathbb{Q}(\sqrt{2})) = \{1, \sigma_2\}$ και $Fix\{1, \sigma_4\} = \mathbb{Q}(\sqrt{6})$.

Διάγραμμα υποσωμάτων του K



Διάγραμμα υποομάδων της G



Έστω $H = \{1, \sigma_4\}$. Ας επαληθεύσουμε ότι $FixH = \mathbb{Q}(\sqrt{6})$. Επειδή

$$\sigma_4(\sqrt{6}) = \sigma_4(\sqrt{2}\sqrt{3}) = \sigma_4(\sqrt{2})\sigma_4(\sqrt{3}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6},$$

έχουμε

$$\mathbb{Q}(\sqrt{6}) \subseteq FixH .$$

Το Θεώρημα 5.3 ii) δίνει $[FixH : \mathbb{Q}] = [G : H] = 2$. Επειδή $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = \deg Irr(\sqrt{6}, \mathbb{Q}) = \deg(x^2 - 6) = 2$, παίρνουμε

$$[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = [FixH : \mathbb{Q}] .$$

Άρα $\mathbb{Q}(\sqrt{6}) = FixH$. Με παρόμοιο τρόπο επαληθεύονται οι υπόλοιπες περιπτώσεις.

Επειδή στο διάγραμμα των υποομάδων της G καταγράφονται όλες οι υποομάδες, από το Θεώρημα 5.3 i) έπεται ότι στο παραπάνω διάγραμμα υποσωμάτων του $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ καταγράφονται όλα τα υποσώματα.

Παράδειγμα 5.6 Έστω $K \subseteq \mathbb{C}$ το σώμα ριζών του $x^3 - 5$ πάνω από το $\mathbb{Q}$. Οι ρίζες του $x^3 - 5$ είναι οι $\rho, \rho\omega, \rho\omega^2$, όπου $\rho = \sqrt[3]{5}$ και $\omega^2 + \omega + 1 = 0$. Άρα $K = \mathbb{Q}(\rho, \rho\omega, \rho\omega^2)$. Επειδή $\omega = \omega\rho/\rho$ έχουμε $K = \mathbb{Q}(\rho, \omega)$. Στο Παράδειγμα 4.3 iii) είδαμε ότι $G = Gal(K, \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_6\}$, όπου τα σ_i ορίζονται από

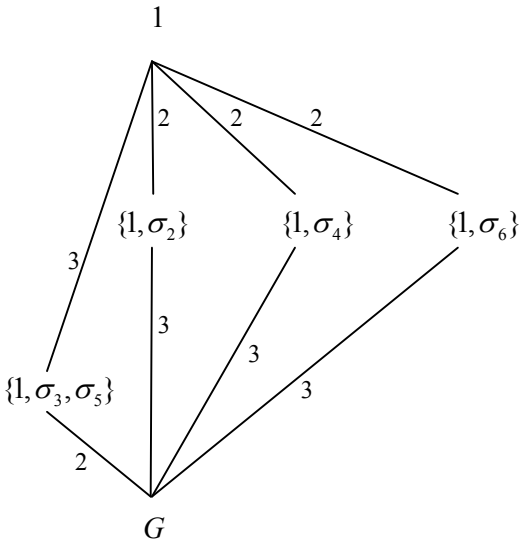
G	$\sigma_i(\rho) = \ldots$	$\sigma_i(\omega) = \ldots$
$\sigma_1 = 1$	ρ	ω
σ_2	ρ	ω^2
σ_3	$\rho\omega$	ω
σ_4	$\rho\omega$	ω^2
σ_5	$\rho\omega^2$	ω
σ_6	$\rho\omega^2$	ω^2

και επίσης είδαμε ότι $G \simeq S_3$. Εύκολα επαληθεύεται ότι οι υποομάδες της G είναι οι

$$1, \{1,\sigma_2\}, \{1,\sigma_4\}, \{1,\sigma_6\}, \{1,\sigma_3,\sigma_5\}, G$$

και το διάγραμμα των υποομάδων της G είναι το ακόλουθο.

Διάγραμμα υποομάδων της $G \simeq S_3$



Στις ακμές σημειώνουμε τους δείκτες διαδοχικών υποομάδων, για παράδειγμα $[G:\{1,\sigma_4\}] = 6/2 = 3$ και $[G:\{1,\sigma_3,\sigma_5\}] = 6/3 = 2$.

Με βάση το παραπάνω διάγραμμα και το Θεώρημα 5.3 μπορούμε να κατασκευάσουμε το διάγραμμα των υποσωμάτων του K υπολογίζοντας το $FixH$ για κάθε υποομάδα H της G. Ας υπολογίσουμε το $FixH$ για $H = \{1,\sigma_2\}$. Μπορούμε να ακολουθήσουμε τη μέθοδο που είδαμε στο Παράδειγμα 5.2 ή αυτή που είδαμε στο προηγούμενο παράδειγμα. Παρατηρούμε ότι αφού $\sigma_2(\rho) = \rho$, έχουμε

$$\mathbb{Q}(\rho) \subseteq FixH .$$

Από το Θεώρημα 5.3 ii),

$$[Fix(H):\mathbb{Q}] = [G:H] = 6/2 = 3 .$$

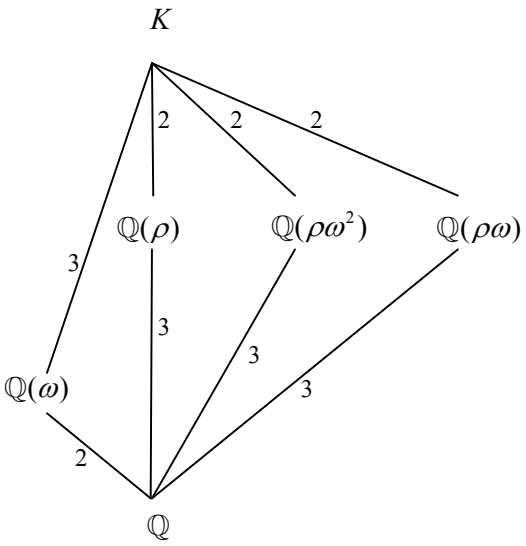
Το πολυώνυμο $x^3 - 5$ είναι ανάγωγο πάνω από $\mathbb{Q}$ και άρα $Irr(\rho,\mathbb{Q}) = x^3 - 5$. Άρα

$$[\mathbb{Q}(\rho):\mathbb{Q}] = 3 = [Fix(H):\mathbb{Q}] .$$

Συνεπώς $\mathbb{Q}(\rho) = FixH$.

Συνεχίζοντας τους υπολογισμούς των σταθερών σωμάτων παίρνουμε το ακόλουθο διάγραμμα υποσωμάτων του K.

Διάγραμμα υποσωμάτων του $K = \mathbb{Q}(\rho,\omega)$



Στις ακμές σημειώνουμε τους βαθμούς διαδοχικών επεκτάσεων, για παράδειγμα $[K:\mathbb{Q}(\rho\omega^2)]=2$ και $[\mathbb{Q}(\rho\omega):\mathbb{Q}]=3$. Από το Θεώρημα 5.3 ii) , οι βαθμοί αυτοί είναι οι αντίστοιχοι δείκτες στο διάγραμμα υποομάδων της G.

Κατά το Θεώρημα 5.3 iii), το $\mathbb{Q}(\rho\omega^2)$ δεν είναι σώμα ριζών πάνω από το $\mathbb{Q}$, αφού η ομάδα $Gal(K,\mathbb{Q}(\rho\omega^2))=\{1,\sigma_4\}$ δεν είναι κανονική στη G (γιατί;).

Παράδειγμα 5.7 Έστω $K\subseteq\mathbb{C}$ το σώμα ριζών του $f(x)=x^4-2$ πάνω από το $\mathbb{Q}$. Θα μελετήσουμε το διάγραμμα υποσωμάτων του K σύμφωνα με το Θεώρημα 5.3.

1) *Η τάξη της* $Gal(K,\mathbb{Q})$.

Οι ρίζες του $f(x)$ είναι οι $\pm\rho,\pm i\rho$, όπου $\rho=\sqrt[4]{2}$, και επομένως $K=\mathbb{Q}(\rho,i\rho)=\mathbb{Q}(\rho,i)$. Από το κριτήριο του Eisenstein το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$. Επομένως

$$[\mathbb{Q}(\rho):\mathbb{Q}]=4.$$

Επειδή $\mathbb{Q}(\rho)\subseteq\mathbb{R}$, το x^2+1 είναι ανάγωγο πάνω από το $\mathbb{Q}(\rho)$ και άρα

$$[\mathbb{Q}(\rho,i):\mathbb{Q}(\rho)]=2.$$

Από το Θεώρημα 1.7

$$[K:\mathbb{Q}]=[K:\mathbb{Q}(\rho)][\mathbb{Q}(\rho):\mathbb{Q}]=2\cdot4=8.$$

Από το Θεώρημα 4.6

$$\left|Gal(K,\mathbb{Q})\right|=8.$$

2) *Τα στοιχεία της* $Gal(K,\mathbb{Q})$.

Αν $\sigma\in Gal(K,\mathbb{Q})$, τότε από $\rho^4=2$ και $i^2=-1$ παίρνουμε

$$\sigma(\rho)\in\{\rho,-\rho,i\rho,-i\rho\}\quad\text{και}\quad\sigma(i)\in\{i,-i\}.$$

Δηλαδή έχουμε συνολικά $4\cdot2=8$ πιθανές περιπτώσεις για το ζεύγος $(\sigma(\rho),\sigma(i))$. Δεδομένου ότι $\left|Gal(K,\mathbb{Q})\right|=8$, συμπεραίνουμε ότι για κάθε $\alpha\in\{\rho,-\rho,i\rho,-i\rho\}$ και κάθε $\beta\in\{i,-i\}$ υπάρχει $\sigma\in Gal(K,\mathbb{Q})$ με $\sigma(\rho)=\alpha,\sigma(i)=\beta$.

Έστω $\sigma,\tau\in Gal(K,\mathbb{Q})$ που ορίζονται από

$$\sigma(i)=i,\ \sigma(\rho)=i\rho,$$
$$\tau(i)=-i,\ \tau(\rho)=\rho.$$

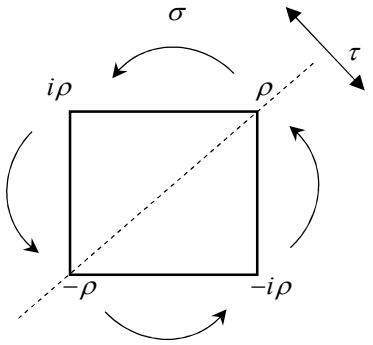
Με πράξεις επαληθεύεται ότι $\sigma^4=\tau^2=1,\ (\sigma\tau)^2=1$ και

$$Gal(K,\mathbb{Q})=\{1,\sigma,\sigma^2,\sigma^3,\tau,\tau\sigma,\tau\sigma^2,\tau\sigma^3\}.$$

Είναι γνωστό[2] ότι από αυτό έπεται ότι $Gal(K,\mathbb{Q})\simeq D_4$, όπου D_4 είναι η διεδρική ομάδα 8 στοιχείων.

Γεωμετρικά, η D_4 είναι η ομάδα των ισομετριών του τετραγώνου. Ας θεωρήσουμε ένα τετράγωνο με κορυφές τις ρίζες $\rho,i\rho,-\rho,,-i\rho$ του x^4-2. Το στοιχείο τ αντιστοιχεί στην ανάκλαση ως προς τη διαγώνιο και το σ παριστάνει στροφή κατά 90^0 όπως στο σχήμα.

[2] Για παράδειγμα, βλ. M. A. Armstrong, Ομάδες και Συμμετρία, ΠΕΚ, 2002, Κεφάλαιο 27.



3) *Το διάγραμμα υποομάδων.*

Αφήνουμε ως άσκηση την επαλήθευση ότι οι υποομάδες της D_4 είναι οι ακόλουθες.

$$\{1\}$$
$$\{1,\tau\},\{1,\tau\sigma^2\},\{1,\sigma^2\},\{1,\tau\sigma\},\{1,\tau\sigma^3\}$$
$$\{1,\tau,\sigma^2,\tau\sigma^2\},\{1,\sigma,\sigma^2,\sigma^3\},\{1,\sigma^2,\tau\sigma,\tau\sigma^3\}$$
$$D_4 .$$

Το διάγραμμα αυτών δίνεται παρακάτω. Σε κάθε ακμή του διαγράμματος ο δείκτης είναι ίσος με 2 (και παραλείπεται από το διάγραμμα).

4) *Το διάγραμμα υποσωμάτων.*

Εφαρμόζοντας την απεικόνιση $Fix(-)$ στο διάγραμμα των υποομάδων της D_4 λαμβάνουμε το διάγραμμα των υποσωμάτων του $\mathbb{Q}(\rho,i)$. Επειδή σε κάθε ακμή του διαγράμματος των υποομάδων ο δείκτης είναι ίσος με 2, σε κάθε ακμή του διαγράμματος υποσωμάτων ο βαθμός είναι 2.

Μένει να καθοριστούν τα σώματα $FixH$ για κάθε υποομάδα H της D_4 και αυτό ενέχει αρκετούς υπολογισμούς. Ας υπολογίσουμε ενδεικτικά δυο περιπτώσεις, πρώτα το $Fix\{1,\sigma^2\}$.

Παρατηρούμε ότι

$$\sigma^2(i) = i ,$$
$$\sigma^2(\rho) = \sigma(i\rho) = i(i\rho) = -\rho ,$$
$$\sigma^2(\rho^2) = (-\rho)^2 = \rho^2 .$$

Συνεπώς $i,\ \rho^2 \in Fix\{1,\sigma^2\}$ και άρα

$$\mathbb{Q}(i,\ \rho^2) \subseteq Fix\{1,\sigma^2\}.$$

Από το Θεώρημα 5.3,

$$[Fix\{1,\sigma^2\}:\mathbb{Q}] = [G:\{1,\sigma^2\}] = 8/2 = 4 .$$

Επειδή $i \notin \mathbb{Q}(\rho^2)$ και $\rho^2 \notin \mathbb{Q}$, έχουμε $[\mathbb{Q}(i,\rho^2):\mathbb{Q}(\rho^2)] \geq 2$ και $[\mathbb{Q}(\rho^2):\mathbb{Q}] \geq 2$. Άρα

$$[\mathbb{Q}(i,\rho^2):\mathbb{Q}] = [\mathbb{Q}(i,\rho^2):\mathbb{Q}(\rho^2)][\mathbb{Q}(\rho^2):\mathbb{Q}] \geq 2\cdot 2 = 4 .$$

Από τα παραπάνω έπεται ότι $\mathbb{Q}(i,\ \rho^2) = Fix\{1,\sigma^2\}$.

Ας βρούμε τώρα το $Fix\{1,\tau\sigma\}$. Αν βρίσκαμε ότι $(1-i)\rho \in Fix\{1,\tau\sigma\}$, τότε όπως πριν θα αποδεικνύαμε ότι $\mathbb{Q}((1-i)\rho) = Fix\{1,\tau\sigma\}$. Όμως πώς σκεφτήκαμε το στοιχείο $(1-i)\rho$; Υπάρχουν διάφοροι τρόποι.

- Θα μπορούσαμε να εφαρμόσουμε την μέθοδο του Παραδείγματος 5.2.
- Αν ξέραμε ότι $Fix\{1,\sigma^2,\tau\sigma,\sigma\tau\} = \mathbb{Q}(i\rho^2)$, τότε από την αντιστοιχία Galois θα είχαμε $[Fix\{1,\tau\sigma\}:\mathbb{Q}(i\rho^2)] = 2$ (βλ. διάγραμμα υποσωμάτων). Συνεπώς θα σκεφτόμασταν τετραγωνικές ρίζες του $i\rho^2$. Παρατηρούμε ότι $((1-i)\rho)^2 = -2i\rho^2$.
- Μια χρήσιμη μέθοδος είναι η εξής. Παρατηρούμε ότι αν $H = \{h_1,...,h_m\} \leq G$, τότε για κάθε $\alpha \in K$ έχουμε

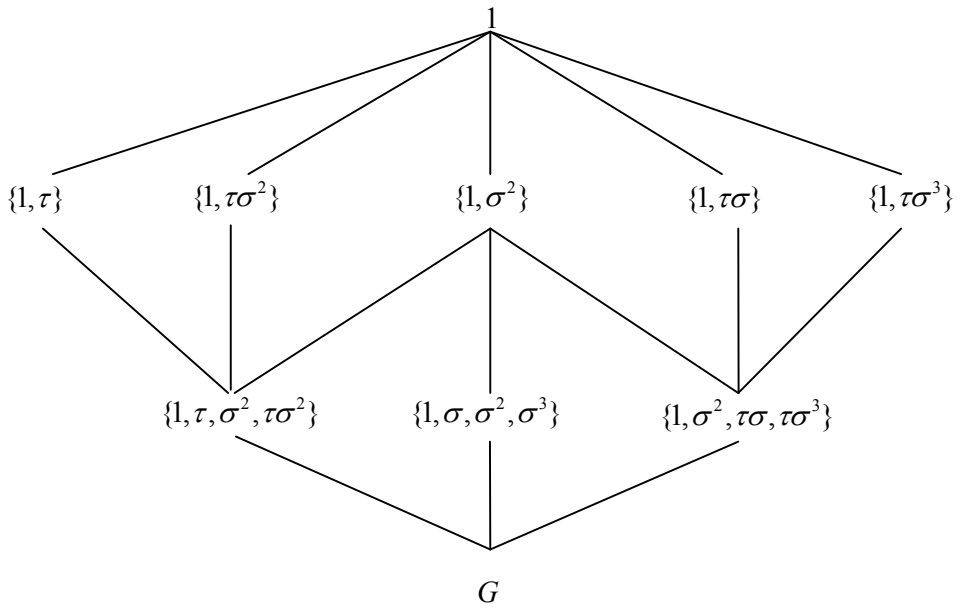
$$h_1(\alpha) + h_2(\alpha) + ... + h_m(\alpha) \in FixH .$$

Γενικά οι συντελεστές του πολυωνύμου

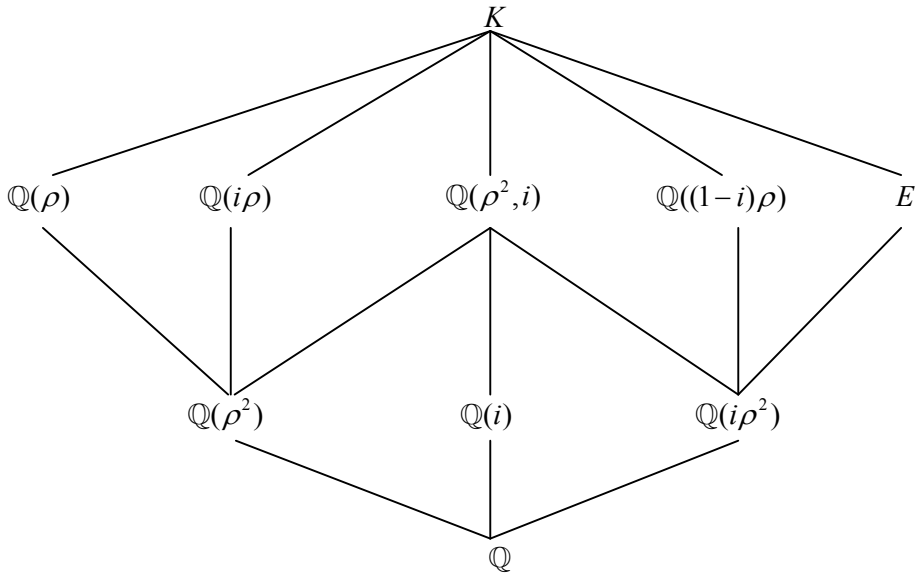
$$(x-h_1(\alpha))(x-h_2(\alpha))...(x-h_m(\alpha))$$

ανήκουν στο $FixH$ (γιατί;). Εδώ έχουμε $H=\{1,\tau\sigma\}$, οπότε $\rho+\tau\sigma(\rho)\in Fix\{1,\tau\sigma\}$. Αλλά $\rho+\tau\sigma(\rho)=\rho-i\rho$.

Διάγραμμα υποομάδων της $D_4=\{1,\sigma,\sigma^2,\sigma^3,\tau,\tau\sigma,\tau\sigma^2,\tau\sigma^3\}$



Διάγραμμα υποσωμάτων του $K=\mathbb{Q}(\rho,i)$



Ο υπολογισμός του E στο παραπάνω διάγραμμα είναι η άσκηση 5.1.

5) *Παραδείγματα που αναφέρονται στο Θεώρημα 5.3 iii).*

Είναι σαφές ότι το $\mathbb{Q}(\rho^2,i)$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$ (του πολυωνύμου $(x^2-2)(x^2+1)$). Από το Θεώρημα 5.3 iii), η υποομάδα $\{1,\sigma^2\}$ είναι κανονική στη G και υπάρχει ισομορφισμός ομάδων

$$G/\{1,\sigma^2\}\simeq Gal(\mathbb{Q}(\rho^2,i),\mathbb{Q}),$$

που επάγεται από την απεικόνιση

$$G\to Gal(\mathbb{Q}(\rho^2,i),\mathbb{Q}),\ \ \varphi\mapsto \text{περιορισμός της } \varphi \text{ στο } \mathbb{Q}(\rho^2,i)\ .$$

Εύκολα επαληθεύεται ότι $G/\{1,\sigma^2\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ και άρα $Gal(\mathbb{Q}(\rho^2,i),\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Τα στοιχεία της $Gal(\mathbb{Q}(\rho^2,i),\mathbb{Q})$ περιγράφονται στον ακόλουθο πίνακα

$Gal(\mathbb{Q}(\rho^2,i),\mathbb{Q})$	$\sigma_j(\sqrt{2}) = \ldots$	$\sigma_j(i)$
1	$\sqrt{2}$	i
$\sigma_2 = \overline{\tau}$	$\sqrt{2}$	$-i$
$\sigma_3 = \overline{\sigma}^2$	$-\sqrt{2}$	i
$\sigma_4 = \overline{\tau}\,\overline{\sigma}^2$	$-\sqrt{2}$	$-i$

όπου με $\overline{\tau}$ και $\overline{\sigma}$ συμβολίζουμε τους περιορισμούς των απεικονίσεων $\tau,\sigma \in G$ στο υποσύνολο $\mathbb{Q}(\rho^2,i)$ του $\mathbb{Q}(\rho,i)$.

Η υποομάδα $\{1,\tau\sigma\}$ δεν είναι κανονική στη G, καθώς $\tau^{-1}(\tau\sigma)\tau = \sigma\tau \notin \{1,\tau\sigma\}$ (γιατί;). Από το Θεώρημα 5.3 iii) έπεται ότι το $\mathbb{Q}((1-i)\rho)$ δεν είναι σώμα ριζών πάνω από $\mathbb{Q}$.

6) *Υποσώματα άλλων σωμάτων.*

Αν κάποιο σώμα E περιέχεται στο παραπάνω διάγραμμα υποσωμάτων, τότε στο διάγραμμα υπάρχουν όλα τα υποσώματα του E. Έτσι έχουμε και το πλήρες διάγραμμα των υποσωμάτων του E. Για παράδειγμα, υπάρχει το διάγραμμα των υποσωμάτων του $\mathbb{Q}((1-i)\rho)$. Ακόμα και αν το E δεν είναι σώμα ριζών, το παραπάνω διάγραμμα περιέχει όλα τα υποσώματά του.

Αν λοιπόν μας δοθεί πεπερασμένη επέκταση E του F, που δεν είναι σώμα ριζών πάνω από το F, ένας τρόπος να βρούμε τα υποσώματα του E είναι να βρούμε επέκταση E' του E (μέσω επισύναψης κατάλληλων ριζών) που είναι σώμα ριζών πάνω από το F και να προσδιορίσουμε τα υποσώματα του E' με την αντιστοιχία Galois.

Εφαρμογή: Η ομάδα Galois πολυωνύμου βαθμού 3

Έστω $x^3+bx^2+cx+d \in \mathbb{Q}[x]$. Κάτω από την αντικατάσταση $x \mapsto x-b/3$, το x^3+bx^2+cx+d μετασχηματίζεται σε πολυώνυμο της μορφής $x^3+px+q \in \mathbb{Q}[x]$ (επαληθεύστε το) και ταυτόχρονα δεν αλλάζει το σώμα ριζών, γιατί το ρ είναι ρίζα του αρχικού πολυωνύμου αν και μόνο αν το $\rho+b/3$ είναι ρίζα του δεύτερου.

Υποθέτουμε ότι $f(x)=x^3+px+q \in \mathbb{Q}[x]$ είναι ανάγωγο. Έστω $K \subseteq \mathbb{C}$ το σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$ και $G = Gal(K,\mathbb{Q})$. Από την Πρόταση 4.10 ξέρουμε ότι η G είναι ισόμορφη με υποομάδα της S_3 και από το Θεώρημα 4.6 ξέρουμε ότι $|G| = [K:\mathbb{Q}]$. Αλλά $[K:\mathbb{Q}] \geq 3$ αφού το $f(x)$ έχει βαθμό 3, είναι ανάγωγο πάνω από το $\mathbb{Q}$ και έχει ρίζα στο K. Άρα $|G| = 3,6$. Επομένως

$$G \simeq S_3 \quad \text{ή} \quad G \simeq A_3,$$

όπου A_3 είναι η υποομάδα της S_3 των άρτιων μεταθέσεων. Στη συνέχεια θα ταυτίζουμε τη G με την S_3 ή A_3 μέσω μεταθέσεων των ριζών. Για παράδειγμα, αν $G \simeq A_3$, θα ταυτίζουμε τη G με την ομάδα

$$\{1, \begin{pmatrix} \rho_1 & \rho_2 & \rho_3 \\ \rho_2 & \rho_3 & \rho_1 \end{pmatrix}, \begin{pmatrix} \rho_1 & \rho_2 & \rho_3 \\ \rho_3 & \rho_1 & \rho_2 \end{pmatrix}\}.$$

Πώς μπορούμε να αποφανθούμε ποιες από τις παραπάνω δυο περιπτώσεις ισχύει; Αν ισχύει $G = S_3$, τότε η G έχει μοναδική υποομάδα δείκτη 2, την A_3, και από το Θεώρημα 5.3 έπεται ότι το K περιέχει μοναδικό υπόσωμα $E = FixA_3$ βαθμού 2 πάνω από το $\mathbb{Q}$. Ποιο είναι το E;

Έστω $\rho_1,\rho_2,\rho_3 \in K$ οι ρίζες του $f(x)$. Θέτουμε

$$\Delta = (\rho_1-\rho_2)(\rho_1-\rho_3)(\rho_2-\rho_3) \in K.$$

Έχουμε $\Delta \neq 0$ αφού οι ρίζες πολυωνύμου που είναι ανάγωγο πάνω από το $\mathbb{Q}$ είναι διακεκριμένες (Πρόταση 0.8).

Παρατηρούμε ότι $\Delta \in FixA_3$. Πράγματι, αν $\tau = \begin{pmatrix} \rho_1 & \rho_2 & \rho_3 \\ \rho_2 & \rho_3 & \rho_1 \end{pmatrix}$, τότε

$$\tau(\Delta) = (\rho_2 - \rho_3)(\rho_2 - \rho_1)(\rho_3 - \rho_1) = (\rho_1 - \rho_2)(\rho_1 - \rho_3)(\rho_2 - \rho_3) = \Delta .$$

Συνεπώς $\tau^2(\Delta) = \Delta$ και $\Delta \in FixA_3$.

Επίσης, αν $\sigma \in S_3$ και $\sigma \notin A_3$, τότε $\sigma(\Delta) = -\Delta$. Για παράδειγμα, αν $\sigma = \begin{pmatrix} \rho_1 & \rho_2 & \rho_3 \\ \rho_2 & \rho_1 & \rho_3 \end{pmatrix}$, τότε

$$\sigma(\Delta) = (\rho_2 - \rho_1)(\rho_2 - \rho_3)(\rho_3 - \rho_1) = -(\rho_1 - \rho_2)(\rho_1 - \rho_3)(\rho_2 - \rho_3) = -\Delta .$$

Άρα ισχύει

$$\tau(\Delta) = \Delta \quad \forall \tau \in A_3$$
$$\sigma(\Delta) = -\Delta \quad \forall \sigma \in S_3 - A_3$$

Από τις προηγούμενες σχέσεις έπεται ότι το Δ^2 παραμένει σταθερό κάτω από τη δράση της G, δηλαδή $\Delta^2 \in Fix(G)$. Άρα $\Delta^2 \in \mathbb{Q}$ σύμφωνα με το Πόρισμα 4.7.

Το Δ^2 ονομάζεται η **διακρίνουσα** του $f(x)$. Αποδεικνύεται ότι

$$\Delta^2 = -4p^3 - 27q^2.$$

Θα δούμε την απόδειξη της σχέσης αυτής μετά.

Θεώρημα 5.8 *Έστω $f(x) = x^3 + px + q \in \mathbb{Q}[x]$ ανάγωγο, $K \subseteq \mathbb{C}$ το σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$ και $G = Gal(K, \mathbb{Q})$.*

i) $G = S_3$ αν και μόνο αν το Δ^2 δεν είναι το τετράγωνο ρητού αριθμού. Στην περίπτωση αυτή το μοναδικό υπόσωμα E του K βαθμού 2 πάνω από το $\mathbb{Q}$ είναι το $E = \mathbb{Q}(\Delta)$.

ii) $G = A_3$ αν και μόνο αν το Δ^2 είναι το τετράγωνο ρητού αριθμού.

iii) Το $f(x)$ έχει ακριβώς μία πραγματική ρίζα αν και μόνο αν $\Delta^2 < 0$.

iv) Το $f(x)$ έχει τρεις πραγματική ρίζες αν και μόνο αν $\Delta^2 > 0$.

Απόδειξη Είδαμε πριν τα εξής.

- $G = S_3$ ή $G = A_3$.
- $\Delta \in FixA_3$.
- Αν $G = S_3$, τότε υπάρχει $\sigma \in G$, με $\sigma(\Delta) \neq \Delta$.

i) Έχουμε $G = S_3 \Leftrightarrow$ υπάρχει $\sigma \in G$ με $\sigma(\Delta) \neq \Delta \Leftrightarrow \Delta \notin FixG \Leftrightarrow \Delta \notin \mathbb{Q} \Leftrightarrow$ το Δ^2 δεν είναι το τετράγωνο ρητού αριθμού. Στην προτελευταία ισοδυναμία χρησιμοποιήσαμε την Πόρισμα 4.7 που λέει ότι $FixG = \mathbb{Q}$.

Έστω $G = S_3$. Επειδή η S_3 περιέχει μοναδική υποομάδα δείκτη 2, από το Θεώρημα 5.3 έπεται ότι το K περιέχει μοναδικό υπόσωμα E βαθμού 2 πάνω από το $\mathbb{Q}$. Έχουμε $[\mathbb{Q}(\Delta) : \mathbb{Q}] \leq 2$ αφού $\Delta^2 \in \mathbb{Q}$ και $[\mathbb{Q}(\Delta) : \mathbb{Q}] > 1$ αφού $\Delta \notin \mathbb{Q}$. Άρα $E = \mathbb{Q}(\Delta)$.

ii) Άμεσο από τα προηγούμενα.

iii) και iv) Το $f(x)$ έχει τουλάχιστον μία πραγματική ρίζα γιατί είναι περιττού βαθμού και έχει πραγματικούς συντελεστές. Αν έχει τρεις πραγματικές ρίζες, τότε $\Delta = (\rho_1 - \rho_2)(\rho_1 - \rho_3)(\rho_2 - \rho_3) \in \mathbb{R}$ και φυσικά $\Delta^2 > 0$. Αν το $f(x)$ έχει μια πραγματική ρίζα ρ_1 και δύο μη πραγματικές ρίζες ρ_2, ρ_3, τότε $\rho_3 = \overline{\rho}_2$ και επομένως

$$\begin{aligned} \Delta &= (\rho_1 - \rho_2)(\rho_1 - \rho_3)(\rho_2 - \rho_3) = \\ &= (\rho_1 - \rho_2)(\rho_1 - \overline{\rho}_2)(\rho_2 - \overline{\rho}_2) = \\ &= |\rho_1 - \rho_2|^2 (\rho_2 - \overline{\rho}_2). \end{aligned}$$

Επειδή $\rho_2 - \overline{\rho}_2 = 2\beta i$, όπου $\beta \in \mathbb{R}$, έχουμε $\Delta^2 = -4\beta^2 \left|\rho_1 - \rho_2\right|^4 < 0$.

Παραδείγματα 5.9

i) Το $x^3 - 3x + 1$ είναι ανάγωγο πάνω από το $\mathbb{Q}$, γιατί είναι τρίτου βαθμού και δεν έχει ρητή ρίζα (Πρόταση 0.1). Η διακρίνουσά του είναι $-4(-3)^3 - 27 = 81$ που είναι τετράγωνο ρητού αριθμού. Άρα η αντίστοιχη ομάδα Galois είναι η A_3. Αφού η διακρίνουσα είναι θετική, το $x^3 - 3x + 1$ έχει τρεις πραγματικές ρίζες.

ii) Το $x^3 + 3x + 1$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ και η διακρίνουσά του είναι $-4 \cdot 3^3 - 27 = -135$. Άρα η αντίστοιχη ομάδα Galois είναι η S_3. Το μοναδικό υπόσωμα E του Θεωρήματος είναι το $\mathbb{Q}(i\sqrt{135})$. Αφού η διακρίνουσα είναι αρνητική, το $x^3 - 3x + 1$ έχει ακριβώς μία πραγματική ρίζα.

Θα δείξουμε τώρα ότι $\Delta^2 = -4p^3 - 27q^2$. Έχουμε $f(x) = (x - \rho_1)(x - \rho_2)(x - \rho_3) = x^3 + px + q$. Άρα

$$e_1 = 0,\ e_2 = p,\ e_3 = -q,$$

όπου

$$e_1 = \rho_1 + \rho_2 + \rho_3,$$
$$e_2 = \rho_1\rho_2 + \rho_1\rho_3 + \rho_2\rho_3,$$
$$e_3 = \rho_1\rho_2\rho_3.$$

Παίρνοντας παράγωγο έχουμε $f'(x) = \sum_{i<j} (x - \rho_i)(x - \rho_j)$ και άρα

$$\begin{aligned}
\Delta^2 &= -f'(\rho_1)f'(\rho_2)f'(\rho_3) = -(3\rho_1^2 + p)(3\rho_2^2 + p)(3\rho_3^2 + p) = \\
&= -\left(27\rho_1^2\rho_2^2\rho_3^2 + 9p(\rho_1^2\rho_2^2 + \rho_1^2\rho_3^2 + \rho_2^2\rho_3^2) + 3p^2(\rho_1^2 + \rho_2^2 + \rho_3^2) + p^3\right) = \\
&= -\left(27e_3^2 + 9p(e_2^2 - 2e_3e_1) + 3p^2(e_1^2 - 2e_2) + p^3\right) = \\
&= -\left(27q^2 + 9p^3 + 3p^2(-2p) + p^3\right) = \\
&= -4p^3 - 27q^2,
\end{aligned}$$

όπου χρησιμοποιήσαμε τις σχέσεις
$\rho_1^2\rho_2^2 + \rho_1^2\rho_3^2 + \rho_2^2\rho_3^2 = (\rho_1\rho_2 + \rho_1\rho_3 + \rho_2\rho_3)^2 - 2(\rho_1^2\rho_2\rho_3 + \rho_1\rho_2^2\rho_3 + \rho_1\rho_2\rho_3^2) = e_2^2 - 2e_3e_1$ και
$\rho_1^2 + \rho_2^2 + \rho_3^2 = (\rho_1 + \rho_2 + \rho_3)^2 - 2(\rho_1\rho_2 + \rho_1\rho_3 + \rho_2\rho_3) = e_1^2 - 2e_2$.

Ασκήσεις 5

Στις επόμενες ασκήσεις το F είναι σώμα χαρακτηριστικής 0.

1. Στο Παράδειγμα 5.7 να βρεθεί ένα a τέτοιο ώστε $E = \mathbb{Q}(a)$.
2. Να βρεθούν όλα τα σώματα E με $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(i\sqrt[4]{2})$.
3. Έστω K σώμα ριζών πάνω από το $\mathbb{Q}$ τέτοιο ώστε $Gal(K, \mathbb{Q}) \simeq S_3$. Δείξτε ότι αν $\sqrt{5} \in K$, τότε $\sqrt{7} \notin K$.
4. Να βρεθεί το διάγραμμα των υποσωμάτων του σώματος ριζών στο $\mathbb{C}$ του $(x^2 - 2)(x^2 + 1)$ πάνω από το $\mathbb{Q}$. Για κάθε ενδιάμεσο σώμα E να βρεθεί ένα a τέτοιο ώστε $E = \mathbb{Q}(a)$.
5. Έστω K σώμα ριζών πάνω από το F τέτοιο ώστε η $Gal(K, F)$ είναι κυκλική τάξης 6. Έστω σ ένας γεννήτορας της G. Δείξτε τα εξής.
   a. Υπάρχει μοναδικό E με $F \subseteq E \subseteq K$ και $[E : F] = 3$. Επίσης υπάρχει μοναδικό L με $F \subseteq L \subseteq K$ και $[L : F] = 2$.
   b. $E \cap L = F$.
   c. Έστω $H = \{1, \sigma^2, \sigma^4\}$. Τότε $FixH = L$ και $Gal(K, L) = H$.

d. Αν $p(x) \in F[x]$ είναι ανάγωγο και έχει μια ρίζα στο E, τότε το $p(x)$ αναλύεται πλήρως στο $E[x]$.

e. Για κάθε $a \in K$ υπάρχουν $e_1,..,e_n \in E$ και $l_1,...,l_n \in L$ με $a = e_1 l_1 + ... + e_n l_n$.

6. Έστω K σώμα ριζών πάνω από το F με $Gal(K,F) \simeq S_4$. Πόσα ενδιάμεσα σώματα E με $[K:E] = 2$ υπάρχουν; Πόσα από αυτά είναι σώματα ριζών πάνω από το F;
7. Έστω $F(a)$ σώμα ριζών πάνω από το F με $F(a) \neq F$. Έστω ότι υπάρχει $\sigma \in Gal(F(a),F)$ τέτοιο ώστε $\sigma(a) = a^{-1}$. Δείξτε ότι $[F(a):F] = 2[F(a+a^{-1}):F]$.
8. Αν το K είναι σώμα ριζών πάνω από το $\mathbb{Q}$ και η $Gal(K,\mathbb{Q})$ είναι κυκλική τάξης 4, τότε $i \notin K$.
9. Έστω $\zeta_7 = \cos(2\pi/7) + i\sin(2\pi/7) \in \mathbb{C}$, $K = \mathbb{Q}(\zeta_7)$ και $G = Gal(K,\mathbb{Q})$.
   a. Ποιο είναι το $Irr(\zeta_7,\mathbb{Q})$ και ποια η τάξη της G;
   b. Δείξτε ότι η G είναι κυκλική και ένας γεννήτορας είναι το $\sigma : K \to K$ που ορίζεται από $\sigma(\zeta_7) = \zeta_7^{\,3}$.
   c. Με το συμβολισμό της άσκησης 3, δείξτε ότι $E = \mathbb{Q}(\zeta_7 + \zeta_7^{\,6})$ και $L = \mathbb{Q}(\zeta_7^{\,3} + \zeta_7^{\,5} + \zeta_7^{\,6})$;
   d. Δείξτε ότι $\mathbb{Q}(\zeta_7 + \zeta_7^{\,6}) = K \cap \mathbb{R}$.
10. Έστω K σώμα ριζών πάνω από το F, $a \in K$, $p(x) = Irr(a,F)$ και $G = Gal(K,F)$.
    a. Δείξτε ότι
    $$\prod_{\sigma \in G} (x - \sigma(a)) = p(x)^m,$$
    όπου $m = [K : F(a)]$.
    b. Βρείτε το $Irr(\zeta_7 + \zeta_7^{\,6},\mathbb{Q})$ και το $Irr(\zeta_7^{\,3} + \zeta_7^{\,5} + \zeta_7^{\,6},\mathbb{Q})$ (βλ. προηγούμενη άσκηση).
11. Έστω $K \subseteq \mathbb{C}$ το σώμα ριζών του $f(x) = x^4 - 4x^2 + 1$ πάνω από το $\mathbb{Q}$, $a = \sqrt{2+\sqrt{3}}$ και $b = \sqrt{2-\sqrt{3}}$.
    a. Δείξτε ότι $K = \mathbb{Q}(a,b) = \mathbb{Q}(a)$.
    b. Δείξτε ότι $Gal(K,\mathbb{Q}) = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, όπου τα σ_i περιγράφονται από τον ακόλουθο πίνακα

$Gal(K,\mathbb{Q})$	$\sigma_i(a) =$
σ_1	a
σ_2	$-a$
σ_3	b
σ_4	$-b$

    c. Αληθεύει ότι η $Gal(K,\mathbb{Q})$ είναι κυκλική;
    d. Να βρεθούν τα διαγράμματα υποομάδων και υποσωμάτων.
    e. Ασαφής ερώτηση: Πώς ερμηνεύετε ότι $\sqrt{2+\sqrt{3}} = \dfrac{\sqrt{2}+\sqrt{6}}{2}$;
12. Έστω K μια πεπερασμένη επέκταση του F. Δείξτε ότι το πλήθος των σωμάτων E με $F \subseteq E \subseteq K$ είναι πεπερασμένο.
13. Έστω $K \subseteq \mathbb{C}$ το σώμα ριζών του $f(x) = x^3 + x + 1$ πάνω από το $\mathbb{Q}$.
    a. Ποια είναι η $Gal(K,\mathbb{Q})$;
    b. Δείξτε ότι $Gal(\mathbb{Q}(a),\mathbb{Q}) = 1$ για κάθε ρίζα a του $f(x)$.
    c. Αληθεύει ότι $i\sqrt{3} \in K$;
    d. Αληθεύει ότι το K περιέχει ρίζα του $x^3 - x + 1$;
14. Έστω $f(x) = x^3 + px + q$ και $g(x) = x^3 + p'x + q'$ δύο ανάγωγα πολυώνυμα πάνω από το $\mathbb{Q}$ με διακρίνουσες -21 και 81 αντίστοιχα. Δείξτε ότι $|Gal(K,\mathbb{Q})| = 18$, όπου $K \subseteq \mathbb{C}$ το σώμα ριζών του $f(x)g(x)$.

15. Έστω K σώμα ριζών πάνω από το $\mathbb{Q}$ τέτοιο ώστε η ομάδα $Gal(K,\mathbb{Q})$ είναι αβελιανή. Δείξτε ότι το x^5-2 είναι ανάγωγο πάνω από το K.
16. Έστω $f(x)\in\mathbb{Q}[x]$ ανάγωγο βαθμού n και K σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$. Δείξτε ότι αν η $Gal(K,\mathbb{Q})$ είναι αβελιανή, τότε $\left|Gal(K,\mathbb{Q})\right|=n$.
17. Έστω $f(x)\in\mathbb{Q}[x]$ ανάγωγο βαθμού p, όπου p πρώτος, και K σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$. Δείξτε τα εξής.
    a. $[K:\mathbb{Q}]=pm$, όπου μκδ$(p,m)=1$.
    b. *[i]Αν υπάρχει κανονική υποομάδα $H\le Gal(K,\mathbb{Q})$ με $\left|H\right|=m$, τότε $m=1$.
18. Εξετάστε ποιες από τις ακόλουθες προτάσεις είναι αληθείς.
    a. Αν K είναι σώμα ριζών πάνω από το $\mathbb{Q}$ με ομάδα Galois ισόμορφη με τη S_n, τότε υπάρχει $a\in K$ με $\deg Irr(a,\mathbb{Q})=n$.
    b. Αν K είναι πεπερασμένη επέκταση του F και $H\le Gal(K,F)$, τότε υπάρχει ενδιάμεσο σώμα E με $Gal(K,E)=H$.
    c. Έστω $\mathbb{Q}\subseteq E\subseteq K$ διαδοχικές επεκτάσεις με $Gal(K,E)=Gal(K,\mathbb{Q})$. Τότε $E=\mathbb{Q}$.
    d. Αν K είναι επέκταση του F και $Gal(K,F)=1$, τότε το K είναι σώμα ριζών πάνω από το F.

[i] Απαιτητική άσκηση. Επιπλέον χρειάζονται γνώσεις από δράσεις ομάδων.

6. Κυκλοτομικά πολυώνυμα, κατασκευάσιμα n-γωνα

Βασικά σημεία

- Ορισμός και υπολογισμός κυκλοτομικών πολυωνύμων.
- Τα κυκλοτομικά πολυώνυμα είναι ανάγωγα πάνω από το $\mathbb{Q}$.
- Η ομάδα Galois του x^n-1 πάνω από το $\mathbb{Q}$ είναι αβελιανή τάξης $\varphi(n)$.
- Θεώρημα του Gauss για κατασκευάσιμα κανονικά πολύγωνα.

Κυκλοτομικά πολυώνυμα

Έστω n θετικός ακέραιος και $K \subseteq \mathbb{C}$ το σώμα ριζών του x^n-1 πάνω από το $\mathbb{Q}$. Ξέρουμε ότι το πολυώνυμο x^n-1 έχει n διακεκριμένες ρίζες στο $\mathbb{C}$ και ότι αυτές είναι οι $1, \zeta_n, \zeta_n^{\,2}, ..., \zeta_n^{\,n-1}$, όπου

$$\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n).$$

Άρα $K = \mathbb{Q}(1, \zeta_n, \zeta_n^{\,2}, ..., \zeta_n^{\,n-1})$ και επομένως

$$K = \mathbb{Q}(\zeta_n).$$

Επίσης ξέρουμε ότι το σύνολο $E_n = \{z \in \mathbb{C} \mid z^n = 1\}$ είναι ομάδα με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών και άρα είναι κυκλική τάξης n

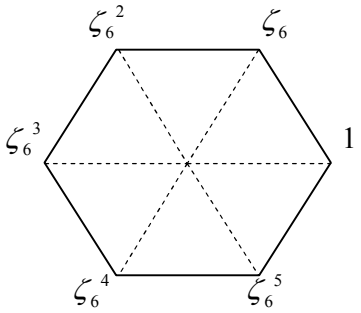
$$E_n = \{1, \zeta_n, \zeta_n^{\,2}, ..., \zeta_n^{\,n-1}\}.$$

Οι γεννήτορες της E_n είναι τα στοιχεία

$$\zeta_n^{\,d}, \text{ όπου } 1 \le d \le n \text{ και } \mu\kappa\delta(d,n) = 1,$$

και το πλήθος τους είναι η τιμή $\varphi(n)$ της συνάρτησης του Euler.

Για παράδειγμα, η ομάδα $E_6 = \{1, \zeta_6, \zeta_6^{\,2}, \zeta_6^{\,3}, \zeta_6^{\,4}, \zeta_6^{\,5}\}$ έχει $\varphi(6) = 2$ γεννήτορες, τους $\zeta_6, \zeta_6^{\,5}$. Στο μιγαδικό επίπεδο, τα σημεία που αντιστοιχούν στους μιγαδικούς αριθμούς $\zeta_n^{\,i}$, $i = 0, ..., n-1$, είναι οι κορυφές κανονικού n-γώνου εγγεγραμμένου στο μοναδιαίο κύκλο, όπως δείχνει το ακόλουθο σχήμα για $n = 6$.



Κάθε γεννήτορας της ομάδας E_n λέγεται **πρωταρχική** n-στη ρίζα της μονάδας. Συνεπώς οι πρωταρχικές n-στες ρίζες της μονάδας είναι τα στοιχεία $\zeta_n^{\,d}$, όπου $1 \le d \le n$ και $\mu\kappa\delta(d,n) = 1$. Παρατηρούμε ότι για κάθε ζ που είναι πρωταρχική n-στη ρίζα της μονάδας έχουμε $K = \mathbb{Q}(\zeta)$.

Ορισμός 6.1 *Το πολυώνυμο*

$$\Phi_n(x) = \prod_{\substack{1 \le d \le n \\ \mu\kappa\delta(d,n)=1}} (x - \zeta_n^{\,d})$$

λέγεται το ***n-στο κυκλοτομικό πολυώνυμο****.*

Παράδειγμα Έστω $n = 8$ και $\zeta = \zeta_8 = \cos(2\pi/8) + i\sin(2\pi/8) = \sqrt{2}/2 + i\sqrt{2}/2$. Τότε

$$\begin{aligned}\Phi_8(x) &= (x-\zeta)(x-\zeta^3)(x-\zeta^5)(x-\zeta^7) = \\ &= (x-\zeta)(x-\zeta^7)(x-\zeta^3)(x-\zeta^5) \\ &= (x-\zeta)(x-\zeta^{-1})(x-\zeta^3)(x-\zeta^{-3}) = \\ &= (x^2-(\zeta+\zeta^{-1})x+1)(x^2-(\zeta^3+\zeta^{-3})x+1) = \\ &= (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1) = \\ &= x^4+1.\end{aligned}$$

Στην προτελευταία ισότητα χρησιμοποιήσαμε ότι $\zeta^k = \cos(2\pi k/8) + i\sin(2\pi k/8)$ κάθε ακέραιο k, σύμφωνα με το θεώρημα de Moivre.

Παρατηρήσεις

- Από τον ορισμό έχουμε ότι το $\Phi_n(x)$ δεν έχει διπλή ρίζα και μάλιστα $\deg \Phi_n(x) = \varphi(n)$.
- Έχομε $\Phi_n(x) \in \mathbb{C}[x]$. Θα δούμε παρακάτω ότι $\Phi_n(x) \in \mathbb{Z}[x]$.
- Αν $\zeta \in E_n$, με $o(\zeta)$ συμβολίζουμε την τάξη του στοιχείου ζ της ομάδας E_n. Συνεπώς το $\zeta \in E_n$ είναι πρωταρχική n-στη ρίζα της μονάδας αν και μόνο αν $o(\zeta) = n$. Επομένως
$$\Phi_n(x) = \prod_{\substack{\zeta \in E_n \\ o(\zeta)=n}} (x-\zeta).$$
- Αν ζ είναι πρωταρχική n-στη ρίζα της μονάδας και $\sigma \in Gal(\mathbb{Q}(\zeta),\mathbb{Q})$, τότε ο περιορισμός της απεικόνισης σ στο E_n δίνει ένα ισομορφισμό ομάδων $E_n \to E_n$ (γιατί;). Άρα το $\sigma(\zeta)$ είναι πρωταρχική n-στη ρίζα της μονάδας.

Πρόταση 6.2 $\Phi_n(x) \in \mathbb{Z}[x]$.

Απόδειξη Αν το ζ είναι πρωταρχική n-στη ρίζα της μονάδας, τότε για κάθε $\sigma \in Gal(\mathbb{Q}(\zeta),\mathbb{Q})$ το $\sigma(\zeta)$ είναι πρωταρχική n-στη ρίζα της μονάδας. Από αυτό και τον ορισμό του $\Phi_n(x)$ έπεται ότι

$$\sigma(\Phi_n(x)) = \Phi_n(x)$$

για κάθε $\sigma \in Gal(\mathbb{Q}(\zeta),\mathbb{Q})$. Άρα οι συντελεστές του $\Phi_n(x)$ ανήκουν στο $Fix(Gal(\mathbb{Q}(\zeta),\mathbb{Q}))$. Όμως από το Πόρισμα 4.7, $Fix(Gal(\mathbb{Q}(\zeta),\mathbb{Q})) = \mathbb{Q}$.

Επειδή το $\Phi_n(x)$ διαιρεί το x^n-1 πάνω από το $\mathbb{C}$, έχουμε ότι το $\Phi_n(x)$ διαιρεί το x^n-1 πάνω από το $\mathbb{Q}$. Επειδή $x^n-1 \in \mathbb{Z}[x]$, $\Phi_n(x) \in \mathbb{Q}[x]$ και το $\Phi_n(x)$ είναι μονικό παίρνουμε $\Phi_n(x) \in \mathbb{Z}[x]$ σύμφωνα με την Παρατήρηση μετά το Λήμμα 0.2.

Πρόταση 6.3 $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Απόδειξη Έστω ζ ρίζα του x^n-1. Τότε το ζ είναι ρίζα του $\Phi_d(x)$, όπου $d = o(\zeta)$. Ξέρουμε ότι το x^n-1 δεν έχει πολλαπλή ρίζα στο $\mathbb{C}$. Άρα το πολυώνυμο x^n-1 διαιρεί το $\prod_{d|n} \Phi_d(x)$.

Αντίστροφα, έστω ζ ρίζα του $\prod_{d|n} \Phi_d(x)$. Τότε το ζ είναι ρίζα κάποιου $\Phi_d(x)$, όπου $d \mid n$, και επομένως $\zeta^n = (\zeta^d)^{n/d} = 1$, δηλαδή το ζ είναι ρίζα του x^n-1. Είναι σαφές ότι το $\prod_{d|n} \Phi_d(x)$ δεν έχει πολλαπλή ρίζα καθώς κάθε n-στη ρίζα της μονάδας είναι πρωταρχική d-στη ρίζα της μονάδας για ακριβώς ένα d και κάθε $\Phi_d(x)$ δεν έχει πολλαπλή ρίζα. Άρα το $\prod_{d|n} \Phi_d(x)$ διαιρεί το x^n-1.

Επειδή τα x^n-1 και $\prod_{d|n} \Phi_d(x)$ είναι μονικά παίρνουμε ότι $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Παρατηρήσεις 6.4

i) Λαμβάνοντας βαθμούς, η Πρόταση 6.3 δίνει $n=\sum_{d|n}\varphi(d)$.

ii) Από την Πρόταση 6.3 παίρνουμε μια άλλη απόδειξη ότι $\Phi_n(x)\in\mathbb{Z}[x]$.
Επαγωγή στο n. Για $n=1$, $\Phi_1(x)=x-1\in\mathbb{Z}[x]$. Έστω ότι $\Phi_m(x)\in\mathbb{Z}[x]$ για κάθε $m<n$. Έχουμε
$$x^n-1=\prod_{d|n}\Phi_d(x)=\Phi_n(x)f(x),\ \text{όπου}\ f(x)=\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)\in\mathbb{Z}[x].$$
Το $f(x)$ είναι μονικό πολυώνυμο και επομένως από την Ευκλείδεια διαίρεση στο $\mathbb{Z}[x]$ υπάρχουν $q(x),r(x)\in\mathbb{Z}[x]$ με $x^n-1=q(x)f(x)+r(x)$ και $\deg r(x)<\deg f(x)$. Από τη σχέση $x^n-1=\Phi_n(x)f(x)$ και τη μοναδικότητα του πηλίκου και του υπολοίπου της Ευκλείδειας διαίρεσης στο $\mathbb{C}[x]$, παίρνουμε $\Phi_n(x)=q(x)\in\mathbb{Z}[x]$.

iii) Η Πρόταση 6.3 μας επιτρέπει να υπολογίζουμε 'αναδρομικά' τα $\Phi_n(x)$. Έχουμε $\Phi_1(x)=x-1$. Άρα:
$$x^2-1=\Phi_1(x)\Phi_2(x)=(x-1)\Phi_2(x)\Rightarrow$$
$$\Rightarrow\Phi_2(x)=x+1,$$
$$x^3-1=\Phi_1(x)\Phi_3(x)=(x-1)\Phi_3(x)\Rightarrow$$
$$\Rightarrow\Phi_3(x)=x^2+x+1,$$
$$x^4-1=\Phi_1(x)\Phi_2(x)\Phi_4(x)=(x-1)(x+1)\Phi_4(x)\Rightarrow$$
$$\Rightarrow\Phi_4(x)=x^2+1,$$
$$x^5-1=\Phi_1(x)\Phi_5(x)=(x-1)\Phi_5(x)\Rightarrow$$
$$\Rightarrow\Phi_5(x)=x^4+x^3+x^2+x+1,$$
$$x^6-1=\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)=(x-1)(x+1)(x^2+x+1)\Phi_6(x)\Rightarrow$$
$$\Rightarrow\Phi_6(x)=x^2-x+1,$$
$$x^7-1=\Phi_1(x)\Phi_7(x)=(x-1)\Phi_7(x)\Rightarrow$$
$$\Rightarrow\Phi_5(x)=x^7+x^6+....+x+1,$$
$$x^8-1=\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)=(x-1)(x+1)(x^2+1)\Phi_8(x)\Rightarrow$$
$$\Rightarrow\Phi_8(x)=x^4+1,$$
$$x^9-1=\Phi_1(x)\Phi_3(x)\Phi_9(x)=(x-1)(x^2+x+1)\Phi_9(x)\Rightarrow$$
$$\Rightarrow\Phi_9(x)=x^6+x^3+1,$$
$$x^{10}-1=\Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)=(x-1)(x+1)(x^4+x^3+x^2+x+1)\Phi_{10}(x)\Rightarrow$$
$$\Rightarrow\Phi_{10}(x)=x^4-x^3+x^2-x+1.$$
Για κάθε πρώτο p, $x^p-1=\Phi_1(x)\Phi_p(x)\Rightarrow\Phi_p(x)=x^{p-1}+x^{p-2}+...+x+1$.

Στο Παράδειγμα 0.5 είδαμε ότι το $\Phi_p(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ για κάθε πρώτο p. Πιο γενικά ισχύει το ακόλουθο αποτέλεσμα.

Θεώρημα 6.5 *Το $\Phi_n(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ για κάθε n.*

Απόδειξη Ξέρουμε ότι $\Phi_n(x)\in\mathbb{Z}[x]$. Από το Λήμμα 0.2 αρκεί να δείξουμε ότι το $\Phi_n(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$. Έστω $f(x)\in\mathbb{Z}[x]$ ανάγωγος μονικός παράγοντας του $\Phi_n(x)$. Επειδή οι ρίζες του $\Phi_n(x)$ είναι απλές και το $\Phi_n(x)$ είναι μονικό, αρκεί να δείξουμε ότι κάθε ρίζα του $\Phi_n(x)$ είναι ρίζα του $f(x)$.

Επειδή το $\Phi_n(x)$ διαιρεί το x^n-1 στο $\mathbb{Z}[x]$, υπάρχει $g(x)\in\mathbb{Z}[x]$ με

$$x^n - 1 = f(x)g(x).$$

Έστω ζ πρωταρχική n-στη ρίζα της μονάδας που είναι ρίζα του $f(x)$ και έστω p πρώτος που δεν διαιρεί το n. Τότε το ζ^p είναι πρωταρχική n-στη ρίζα της μονάδας και φυσικά

$$0 = f(\zeta^p)g(\zeta^p).$$

Ισχυρισμός: $f(\zeta^p) = 0$.

Αν αληθεύει ο ισχυρισμός, τότε με επαναληπτική χρήση αυτού παίρνουμε ότι αν $p_1, ..., p_t$ είναι πρώτοι που δεν διαιρούν το n, τότε $f(\zeta^{p_1 \cdots p_t}) = 0$. Αλλά κάθε πρωταρχική n-στη ρίζα της μονάδας είναι της μορφής $\zeta^{p_1 \cdots p_t}$, δηλαδή κάθε ρίζα του $\Phi_n(x)$ είναι ρίζα του $f(x)$, που είναι το ζητούμενο.

Απόδειξη του ισχυρισμού: Έστω $f(\zeta^p) \neq 0$. Τότε $g(\zeta^p) = 0$. Επειδή το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$, το $f(x)$ διαιρεί το $g(x^p)$ στο $\mathbb{Q}[x]$ και επειδή το $f(x)$ είναι μονικό, το $f(x)$ διαιρεί το $g(x^p)$ στο $\mathbb{Z}[x]$. Άρα

$$g(x^p) = f(x)h(x),$$

όπου $h(x) \in \mathbb{Z}[x]$. Παίρνοντας αναγωγές modulo p (βλ. Ενότητα 0), έχουμε στο $\mathbb{Z}_p[x]$

$$\overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$$

Όμως στο $\mathbb{Z}_p[x]$ ισχύει $\overline{g}(x^p) = (\overline{g}(x))^p$ σύμφωνα με την άσκηση 6.1. Άρα $\mu\kappa\delta(\overline{f}(x), \overline{g}(x)) \neq 1$. Από τη σχέση

$$x^n - 1 = \overline{f}(x)\overline{g}(x)$$

έπεται ότι το $x^n - 1 \in \mathbb{Z}_p[x]$ έχει πολλαπλή ρίζα σε κάποια επέκταση του $\mathbb{Z}_p$. Επειδή το p δεν διαιρεί το n, αυτό είναι αδύνατο λόγω του Παραδείγματος 0.7.

Το προηγούμενο θεώρημα λέει ότι για κάθε πρωταρχική n-στη ρίζα ζ της μονάδας

$$Irr(\zeta, \mathbb{Q}) = \Phi_n(x) \text{ και } [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n).$$

Πρόταση 6.6 *Η ομάδα $Gal(\mathbb{Q}(\zeta), \mathbb{Q})$, όπου ζ είναι πρωταρχική n-στη ρίζα της μονάδας, είναι ισόμορφη με την ομάδα $U(\mathbb{Z}_n)$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_n$. Ειδικά, η $Gal(\mathbb{Q}(\zeta), \mathbb{Q})$ είναι αβελιανή τάξης $\varphi(n)$.*

Απόδειξη Έστω ζ μια πρωταρχική n-στη ρίζα της μονάδας. Αν $\sigma \in Gal(\mathbb{Q}(\zeta), \mathbb{Q})$, τότε

$$\sigma(\zeta) = \zeta^{d_\sigma}$$

για κάποιο ακέραιο d_σ. Επειδή το ζ είναι πρωταρχική n-στη ρίζα της μονάδας, το $\sigma(\zeta) = \zeta^{d_\sigma}$ είναι επίσης πρωταρχική ρίζα n-στη ρίζα της μονάδας και άρα $\mu\kappa\delta(d_\sigma, n) = 1$. Συνεπώς η κλάση $[d_\sigma]$ του d_σ modulo n ανήκει στο $U(\mathbb{Z}_n)$.

Έστω $G = Gal(\mathbb{Q}(\zeta), \mathbb{Q})$. Η απεικόνιση

$$f : G \to U(\mathbb{Z}_n),\ \sigma \mapsto [d_\sigma],$$

είναι ομομορφισμός ομάδων. Πράγματι, αν $\sigma, \tau \in G$, τότε

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{d_\tau}) = \sigma(\zeta)^{d_\tau} = (\zeta^{d_\sigma})^{d_\tau} = \zeta^{d_\sigma d_\tau}.$$

Άρα $f(\sigma\tau) = f(\sigma)f(\tau)$. Η f είναι μονομορφισμός γιατί αν $[d_\sigma] = [1]$, τότε $d_\sigma \equiv 1 \bmod n$ και άρα $\sigma(\zeta) = \zeta^{d_\sigma} = \zeta^1 = \zeta$, δηλαδή η σ είναι η ταυτοτική απεικόνιση $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$.

Μέχρι στιγμής έχουμε ένα μονομορφισμό ομάδων $f : G \to U(\mathbb{Z}_n)$. Επειδή το $\mathbb{Q}(\zeta)$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$, έχουμε

$$|G| = [\mathbb{Q}(\zeta) : \mathbb{Q}]$$

σύμφωνα με το Θεώρημα 4.6. Από το Θεώρημα 6.2,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n(x) = \varphi(n).$$

Επειδή $|U(\mathbb{Z}_n)| = \varphi(n)$, η απεικόνιση $f : G \to U(\mathbb{Z}_n)$ είναι ισομορφισμός.

Παρατήρηση Σύμφωνα με ένα κλασσικό αποτέλεσμα του Gauss[1], η ομάδα $U(\mathbb{Z}_n)$ είναι κυκλική αν και μόνο αν $n = 2, 4, p^k, 2p^k$ όπου p περιττός πρώτος. Συνεπώς ακριβώς για τις τιμές αυτές η $Gal(\mathbb{Q}(\zeta_n), \mathbb{Q})$ είναι κυκλική.

Παράδειγμα 6.7 Έστω $\zeta = \zeta_{24}$ και $G = Gal(\mathbb{Q}(\zeta), \mathbb{Q})$. Θα περιγράψουμε τη G με τρεις τρόπους και θα βρούμε το $Irr(\cos(\pi/12), \mathbb{Q})$.

Επειδή $\mu\kappa\delta(3,8) = 1$ υπάρχει ισομορφισμός δακτυλίων[2] $\mathbb{Z}_{24} \simeq \mathbb{Z}_3 \times \mathbb{Z}_8$ και επομένως υπάρχει ισομορφισμός ομάδων $U(\mathbb{Z}_{24}) \simeq U(\mathbb{Z}_3) \times U(\mathbb{Z}_8)$. Έχουμε $U(\mathbb{Z}_3) \simeq \mathbb{Z}_2$. Με πράξεις εύκολα επαληθεύεται ότι η ομάδα $U(\mathbb{Z}_8)$ δεν είναι κυκλική. Επειδή $|U(\mathbb{Z}_8)| = \varphi(8) = 4$, έχουμε $U(\mathbb{Z}_8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Από την Πρόταση 6.6,

$$G \simeq U(\mathbb{Z}_{24}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Οι πρωταρχικές 24-στες ρίζες της μονάδας είναι οι

$$\zeta^d,\ d = 1,5,7,11,13,17,19,23.$$

Για καθεμιά από τις τιμές αυτές του d έχουμε $\sigma_d \in G$, όπου $\sigma_d(\zeta) = \zeta^d$. Άρα η G είναι το σύνολο αυτών των σ_d.

Παρατηρούμε ότι $\zeta^6 = \cos(2\pi 6/24) + i\sin(2\pi 6/24) = i$ και όμοια $\zeta^3 = \sqrt{2}/2 + i\sqrt{2}/2$, $\zeta^8 = -\sqrt{3}/2 + i\sqrt{3}/2$. Άρα $\zeta^{-3} = \sqrt{2}/2 - i\sqrt{2}/2$, $\zeta^{-8} = -\sqrt{3}/2 - i\sqrt{3}/2$. Όλα τα στοιχεία αυτά ανήκουν στο $K = \mathbb{Q}(\zeta)$. Άρα $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) \subseteq K$. Από την Πρόταση 6.6 έχουμε $[K : \mathbb{Q}] = \varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8$. Αφήνουμε σαν άσκηση την επαλήθευση ότι $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}] = 8$. Άρα

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = K.$$

Συνεπώς το K είναι το σώμα ριζών του $(x^2 - 2)(x^2 - 3)(x^2 + 1)$ πάνω από το $\mathbb{Q}$. Από το Θεώρημα 4.6 $|G| = [K : \mathbb{Q}] = 8.$ Για κάθε $\sigma \in G$ έχουμε

$$\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\},$$
$$\sigma(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\},$$
$$\sigma(i) \in \{i, -i\}$$

σύμφωνα με την Πρόταση 4.2 i). Δεδομένου ότι $|G| = 8$, έπεται ότι για κάθε $\alpha \in \{\sqrt{2}, -\sqrt{2}\}$, $\beta \in \{\sqrt{3}, -\sqrt{3}\}$, $\gamma \in \{i, -i\}$ υπάρχει $\sigma \in G$ με

$$\sigma(\sqrt{2}) = \alpha,$$
$$\sigma(\sqrt{3}) = \beta,$$
$$\sigma(i) = \gamma$$

και αυτά τα σ εξαντλούν το σύνολο G. Άρα $G = \{\sigma_1, \sigma_2, ..., \sigma_8\}$, όπου τα σ_i ορίζονται στον ακόλουθο πίνακα.

[1] Βλ. Εφαρμογή 4.8.3 στο *Μια Εισαγωγή στην Άλγεβρα*, Δ. Βάρσος et al, Γ΄Έκδοση, Εκδόσεις Σοφία 2012.
[2] Βλ. σελίδα 132, *Μια Εισαγωγή στην Άλγεβρα*, Δ. Βάρσος et al, Γ΄Έκδοση, Εκδόσεις Σοφία, 2012.

G	$\sigma_k(\sqrt{2})=$	$\sigma_k(\sqrt{3})=$	$\sigma_k(i)=$
σ_1	$\sqrt{2}$	$\sqrt{3}$	i
σ_2	$\sqrt{2}$	$\sqrt{3}$	$-i$
σ_3	$\sqrt{2}$	$-\sqrt{3}$	i
σ_4	$\sqrt{2}$	$-\sqrt{3}$	$-i$
σ_5	$-\sqrt{2}$	$\sqrt{3}$	i
σ_6	$-\sqrt{2}$	$\sqrt{3}$	$-i$
σ_7	$-\sqrt{2}$	$-\sqrt{3}$	i
σ_8	$-\sqrt{2}$	$-\sqrt{3}$	$-i$

Ας υπολογίσουμε τώρα το $Irr(\cos(\pi/12),\mathbb{Q})$. Χρησιμοποιώντας τη μέθοδο που είδαμε στην Παρατήρηση 6.4 ii) και μετά από μερικές πράξεις βρίσκουμε $\Phi_{12}(x)=x^4-x^2+1$ και με βάση αυτό παίρνουμε $\Phi_{24}(x)=x^8-x^4+1$. Άρα

$$\zeta^8-\zeta^4+1=0\Rightarrow\zeta^4+\zeta^{-4}=1.$$

Χρησιμοποιώντας το διωνυμικό ανάπτυγμα βρίσκουμε

$$\zeta^4+\zeta^{-4}=(\zeta+\zeta^{-1})^4-4(\zeta^2+\zeta^{-2})-6,$$
$$\zeta^2+\zeta^{-2}=(\zeta+\zeta^{-1})^2-2.$$

Άρα το $\zeta+\zeta^{-1}$ είναι ρίζα του x^4-4x^2+1. Επειδή $\zeta+\zeta^{-1}=2\cos(\pi/12)$, το $\cos(\pi/12)$ είναι ρίζα του $f(x)=x^4-x^2+1/16\in\mathbb{Q}[x]$. Για να δείξουμε ότι $Irr(\cos(\pi/12),\mathbb{Q})=f(x)$ αρκεί να δείξουμε ότι $\deg Irr(\cos(\pi/12),\mathbb{Q})=4$.

Θεωρούμε τις διαδοχικές επεκτάσεις

$$\mathbb{Q}\subseteq\mathbb{Q}(\cos(\pi/12))\subseteq\mathbb{Q}(\zeta).$$

Ξέρουμε ότι $[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(24)=8$. Από $2\cos(\pi/12)=\zeta+\zeta^{-1}$ παίρνουμε ότι το ζ είναι ρίζα του $x^2-2\cos(\pi/12)x+1\in\mathbb{Q}(\cos(\pi/12))[x]$. Από αυτό και το ότι $\mathbb{Q}(\cos(\pi/12))\subseteq\mathbb{R}$ και $\mathbb{Q}(\zeta)\not\subseteq\mathbb{R}$ έπεται ότι

$$x^2-2\cos(\pi/12)x+1=Irr(\zeta,\mathbb{Q}(\cos(\pi/12)).$$

Άρα $[\mathbb{Q}(\zeta):\mathbb{Q}(\cos(\pi/12))]=2$. Συνεπώς $\deg Irr(\cos(\pi/12),\mathbb{Q})=[\mathbb{Q}(\cos(\pi/12)):\mathbb{Q}]=8/2=4.$

Ο υπολογισμός του $Irr(\cos(\pi/12),\mathbb{Q})$ που είδαμε πριν, έγινε με τρόπο που υποδεικνύει ότι είναι γενικός. Πιο ειδικά, δηλαδή για το συγκεκριμένο $\zeta=\zeta_{24}$, θα μπορούσαμε να πούμε ότι από $\cos(2\pi/12)=\sqrt{3}/2$ έπεται ότι $2\cos^2(\pi/12)-1=\sqrt{3}/2$ λόγω της ταυτότητας $2\cos^2\theta-1=\cos(2\theta)$, και να υψώσουμε στο τετράγωνο για να βρούμε το πολυώνυμο $16x^4-16x^2+1$ που έχει ρίζα το $\cos(\pi/12)$.

Σημείωση. Τα παραπάνω συνδέονται με τα πολυώνυμα Chebyshev πρώτου είδους, δηλαδή τα πολυώνυμα που προκύπτουν εκφράζοντας το $\cos(n\theta)$ ως πολυώνυμο του $\cos\theta$.

Παράδειγμα 6.8 Θα δείξουμε ότι υπάρχει $f(x)\in\mathbb{Q}[x]$ βαθμού 5 με κυκλική ομάδα Galois τάξης 5.

Για παράδειγμα, ας θεωρήσουμε το σώμα $\mathbb{Q}(\zeta)$, όπου $\zeta=\zeta_{11}$. Τότε $[\mathbb{Q}(\zeta):\mathbb{Q}]=10=\left|Gal(\mathbb{Q}(\zeta),\mathbb{Q})\right|$. Επειδή το 2 είναι πρώτος και $2\big|10$, η $G=Gal(\mathbb{Q}(\zeta),\mathbb{Q})$ έχει υποομάδα H τάξης 2, οπότε από την αντιστοιχία Galois, $[Fix(H):\mathbb{Q}]=10/2=5$. Επειδή η G είναι αβελιανή, κάθε υποομάδα της είναι κανονική. Από το Θεώρημα 5.3, $Gal(FixH,\mathbb{Q})\simeq G/Gal(K,Fix(H))=G/H$ και άρα $\left|Gal(FixH,\mathbb{Q})\right|=5$. Επειδή το 5 είναι πρώτος έχουμε $Gal(FixH,\mathbb{Q})\simeq\mathbb{Z}_5$. Από το Θεώρημα 2.6 υπάρχει $a\in FixH$ με $FixH=\mathbb{Q}(a)$. Τότε το $f(x)=Irr(a,\mathbb{Q})$ έχει βαθμό 5 και ομάδα Galois ισόμορφη με τη $\mathbb{Z}_5$.

Ας υπολογίσουμε τώρα το $f(x)$. Εύκολα επαληθεύεται ότι $G =< \sigma >$, όπου $\sigma(\zeta) = \zeta^2$. Επειδή η G είναι κυκλική και το 2 διαιρεί την τάξη της, η G έχει μοναδική υποομάδα τάξης 2. Από την αντιστοιχία Galois, υπάρχει μοναδικό E με $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\zeta)$ και $[E:\mathbb{Q}] = 5$. Όπως ακριβώς στο προηγούμενο παράδειγμα, εύκολα επαληθεύεται ότι $[\mathbb{Q}(\zeta):\mathbb{Q}(\zeta+\zeta^{-1})] = 2$ και άρα

$$[\mathbb{Q}(\zeta+\zeta^{-1}):\mathbb{Q}] = 5.$$

Συνεπώς

$$E = \mathbb{Q}(\zeta+\zeta^{-1}).$$

Έστω $a = \zeta + \zeta^{-1}$, οπότε $\deg Irr(a,\mathbb{Q}) = 5$. Για να βρούμε το $f(x) = Irr(a,\mathbb{Q})$ υπολογίζουμε διαδοχικά με τη βοήθεια του διωνυμικού αναπτύγματος:

$\zeta + \zeta^{-1} = a$

$\zeta^2 + \zeta^{-2} = (\zeta+\zeta^{-1})^2 - 2 = a^2 - 2$

$\zeta^3 + \zeta^{-3} = (\zeta+\zeta^{-1})^3 - 3(\zeta+\zeta^{-1}) = a^3 - 3a$

$\zeta^4 + \zeta^{-4} = (\zeta+\zeta^{-1})^4 - 4(\zeta^2+\zeta^{-2}) - 6 = a^4 - 4(a^2-2) - 6$

$\zeta^5 + \zeta^{-5} = (\zeta+\zeta^{-1})^5 - 5(\zeta^3+\zeta^{-3}) - 10(\zeta+\zeta^{-1}) = a^5 - 5(a^3-3a) - 10a.$

Επειδή $\zeta^{11} - 1 = 0$, έχουμε $\zeta^{10} + \zeta^9 + ... + \zeta + 1 = 0,$ δηλαδή

$$\zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \zeta^3 + \zeta^{-3} + \zeta^4 + \zeta^{-4} + \zeta^5 + \zeta^{-5} + 1 = 0.$$

Αντικαθιστώντας τις παραπάνω σχέσεις παίρνουμε

$$a^5 + a^4 - 4a^3 - 3a^2 + 3a + 1 = 0.$$

Επειδή ξέρουμε ότι $\deg Irr(a,\mathbb{Q}) = 5$, παίρνουμε ότι $Irr(a,\mathbb{Q}) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$.

Παράδειγμα 6.9 Θα βρούμε το διάγραμμα των υποσωμάτων του $K = \mathbb{Q}(\zeta)$, όπου ζ είναι μια πρωταρχική 13-η ρίζα της μονάδας. Επίσης θα υπολογίσουμε διάφορα ελάχιστα πολυώνυμα.

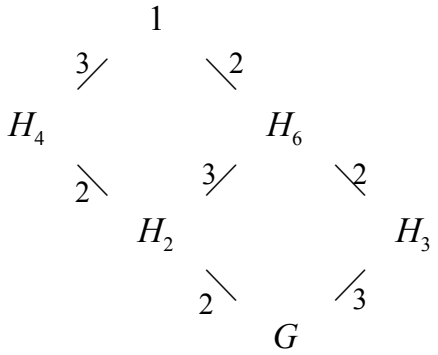
Έστω G η ομάδα Galois του $x^{13} - 1$ πάνω από το $\mathbb{Q}$. Ξέρουμε ότι $|G| = \varphi(13) = 12$ και υπάρχει 1-1 και επί αντιστοιχία $G \to \{1,2,...,12\}$ τέτοια ώστε για κάθε $\sigma \in G$ υπάρχει $k_\sigma \in \{1,2,...,12\}$ με $\sigma(\zeta) = \zeta^{k_\sigma}$. Έστω $\sigma \in G$ που ορίζεται από $\sigma(\zeta) = \zeta^2$. Τότε[3]

$$\sigma^k(\zeta) = \zeta^{2^k}$$

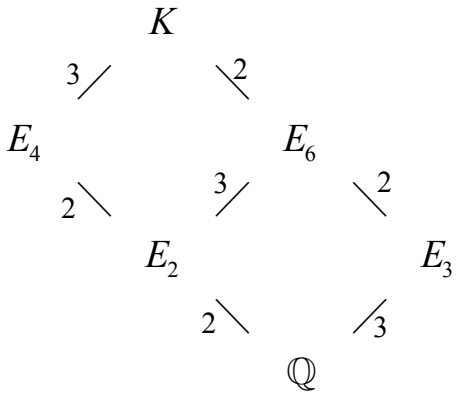
για κάθε θετικό ακέραιο k. Ειδικά $\sigma^4(\zeta) = \zeta^{2^4} = \zeta^3$ αφού $2^4 \equiv 3 \bmod 13$ και επίσης $\sigma^6(\zeta) = \zeta^{2^6} = \zeta^{12}$ αφού $2^6 \equiv 12 \bmod 13$. Επειδή το ζ είναι πρωταρχική 13-η ρίζα της μονάδας έχουμε $\zeta^3 \neq \zeta$ και $\zeta^{12} \neq \zeta$. Συνεπώς τα σ^4 και σ^6 είναι διάφορα της ταυτοτικής απεικόνισης $K \to K$ και επομένως η τάξη του στοιχείου σ στην ομάδα G είναι 12. Άρα η G είναι κυκλική και $G =< \sigma >$.

Ξέρουμε ότι οι υποομάδες πεπερασμένης κυκλικής ομάδας είναι σε 1-1 και επί αντιστοιχία με τους θετικούς διαιρέτες της τάξης της ομάδας. Επίσης, αν $H \leq G$ με $|H| = 12/d$, τότε $H =< \sigma^d >$. Άρα το διάγραμμα των υποομάδων της G είναι το ακόλουθο

[3] Γράφοντας ζ^{2^k} εννούμε $\zeta^{(2^k)}$.



όπου $H_i =< \sigma^i >$. Από την αντιστοιχία Galois, το διάγραμμα των υποσωμάτων του K είναι το ακόλουθο, όπου $E_i = FixH_i$.



Τώρα θα βρούμε ένα γεννήτορα για κάθε ενδιάμεσο σώμα. Αν $H \le G$, θέτουμε

$$a_H = \sum_{h \in H} h(\zeta) .$$

Παρατηρούμε ότι

$$a_H \in FixH ,$$

γιατί για κάθε $h_1 \in H$ ισχύει

$$h_1(a_H) = \sum_{h \in H} h_1 h(\zeta) = \sum_{h \in H} h(\zeta) = a_H ,$$

όπου στη μεσαία ισότητα χρησιμοποιήσαμε ότι αν το h διατρέχει τα στοιχεία της ομάδας H το ίδιο συμβαίνει για το $h_1 h$. Ας θέσουμε $a_i = a_H$ αν $H =< \sigma^i >$. Υπολογίζουμε τα στοιχεία a_i για κάθε υποομάδα H της G. Για $H_2 =< \sigma^2 >= \{1, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}\}$ έχουμε

$$\begin{aligned} a_2 &= \zeta + \sigma^2(\zeta) + \sigma^4(\zeta) + \sigma^6(\zeta) + \sigma^8(\zeta) + \sigma^{10}(\zeta) = \\ &= \zeta + \zeta^{2^2} + \zeta^{2^4} + \zeta^{2^6} + \zeta^{2^8} + \zeta^{2^{10}} = \\ &= \zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10}. \end{aligned}$$

Όμοια βρίσκουμε

$$\begin{aligned} a_3 &= \zeta + \zeta^8 + \zeta^{12} + \zeta^5, \\ a_4 &= \zeta + \zeta^3 + \zeta^9, \\ a_6 &= \zeta + \zeta^{12}. \end{aligned}$$

Μέχρι στιγμής βρήκαμε στοιχεία a_i τέτοια ώστε $\mathbb{Q}(a_i) \subseteq FixH_i,\ i = 2,3,4,6.$ Θα δούμε τώρα ότι σε κάθε περίπτωση ισχύει η ισότητα. Ας δώσουμε δύο αποδείξεις.

1ος τρόπος. Θα χρησιμοποιήσουμε ένα επιχείρημα που εφαρμόζει σε κάθε σώμα $\mathbb{Q}(\zeta)$, όπου ζ πρωταρχική p-στη ρίζα της μονάδας, p πρώτος, και αποφεύγει υπολογισμούς.

Υποθέτουμε λοιπόν ότι το ζ είναι πρωταρχική p-στη ρίζα της μονάδας, p πρώτος. Τα στοιχεία $1,\zeta,\zeta^2,...,\zeta^{p-2}$ είναι βάση του $\mathbb{Q}(\zeta)$ ως $\mathbb{Q}$-διανυσματικός χώρος σύμφωνα με την Πρόταση 1.5. Εύκολα επαληθεύεται ότι τα στοιχεία

$$\zeta,\zeta^2,...,\zeta^{p-2},\zeta^{p-1} \tag{1}$$

είναι βάση του $\mathbb{Q}(\zeta)$ (πώς;). Η ομάδα Galois $G=Gal(\mathbb{Q}(\zeta),\mathbb{Q})$ μεταθέτει τα παραπάνω στοιχεία.

Έστω $H\le G$ και $a_H=\sum_{h\in H}h(\zeta)$. Τότε $a_H\in FixH$ όπως είδαμε πιο πάνω, οπότε $\mathbb{Q}(a_H)\subseteq FixH$. Αν $\mathbb{Q}(a_H)\neq FixH$, τότε από την αντιστοιχία Galois η $Gal(\mathbb{Q}(\zeta),FixH)=H$ περιέχεται γνήσια στην $Gal(\mathbb{Q}(\zeta),\mathbb{Q}(a_H))$, δηλαδή υπάρχει $\tau\in G-H$ με $\tau(a_H)=a_H$. Το $\tau(\zeta)$ είναι στοιχείο της βάσης (1) και εμφανίζεται με συντελεστή 1 στην παράσταση του $\tau(a_H)$ ως γραμμικός συνδυασμός των στοιχείων της βάσης (1). Άρα το $\tau(\zeta)$ εμφανίζεται με συντελεστή 1 στην παράσταση του a_H ως γραμμικός συνδυασμός των στοιχείων της βάσης (1). Άρα $\tau(\zeta)=h(\zeta)$ για κάποιο $h\in H$. Επειδή το ζ παράγει το σώμα $\mathbb{Q}(\zeta)$, έχουμε $\tau=h$. Δηλαδή $\tau\in H$, άτοπο. Άρα $\mathbb{Q}(a_H)=FixH$.

2ος τρόπος. Επειδή έχουμε $\mathbb{Q}(a_i)\subseteq FixH_i$, αρκεί να δείξουμε ότι $\deg Irr(a_i,\mathbb{Q})\ge[FixH_i:\mathbb{Q}]=[G:H_i]$. Επειδή η ομάδα G είναι αβελιανή, κάθε υποομάδα της είναι κανονική. Συνεπώς, από τη Θεώρημα 5.3 ξέρουμε ότι το $FixH_i$ είναι σώμα ριζών άνω από το $\mathbb{Q}$. Επειδή η G παράγεται από το σ, το Θεώρημα 5.3 iii) δίνει ότι η ομάδα Galois της επέκτασης $\mathbb{Q}\subseteq FixH_i$ παράγεται από το $\bar\sigma$, όπου $\bar\sigma$ είναι ο περιορισμός της σ στο $FixH_i$. Εεπιδή το a_i είναι ρίζα του $Irr(a_i,\mathbb{Q})$, κάθε $\bar\sigma^k(a_3)$ είναι ρίζα του $Irr(a_3,\mathbb{Q})$, $k=1,2,...$. Υπολογίζουμε τα στοιχεία $\sigma(a_i),\sigma^2(a_i),\sigma^3(a_i),...$ για $i=3$. Έχουμε

$$\sigma(a_3)=\zeta^2+\zeta^3+\zeta^{11}+\zeta^{10},$$
$$\sigma^2(a_3)=\zeta^4+\zeta^6+\zeta^9+\zeta^7.$$

Βλέπουμε ότι τα στοιχεία $a_3,\sigma(a_3),\sigma^2(a_3)$ είναι διακεκριμένα και επομένως $\deg Irr(a_3,\mathbb{Q})\ge 3=[G:H_3]$. Όμοια αποδεικνύονται και οι άλλες περιπτώσεις.

Επιστρέφοντας στο διάγραμμα υποσωμάτων, έχουμε δείξει ότι $E_i=\mathbb{Q}(a_i)$, $i=2,3,4,6$.

Χρησιμοποιώντας το Πόρισμα 4.5 μπορούμε να βρούμε τα $Irr(\zeta,E_i)$ για κάθε i. Για παράδειγμα,

$$Irr(\zeta,E_3)=\prod_{h\in H_3}(x-h(\zeta))=$$
$$=(x-\zeta)(x-\sigma^3(\zeta))(x-\sigma^6(\zeta))(x-\sigma^9(\zeta))=$$
$$=(x-\zeta)(x-\zeta^8)(x-\zeta^{12})(x-\zeta^5).$$

Επίσης μπορούμε να βρούμε τα ελάχιστα πολυώνυμα των a_i πάνω από διάφορα σώματα. Ας βρούμε το $Irr(a_3,\mathbb{Q})$. Όπως είδαμε στον 2ο τρόπο πριν, το E_3 είναι σώμα ριζών άνω από το $\mathbb{Q}$. Η ομάδα Galois της επέκτασης $\mathbb{Q}\subseteq E_3$ είναι η $Gal(E_3,\mathbb{Q})=\{1,\bar\sigma,\bar\sigma^2\}$, όπου $\bar\sigma$ είναι ο περιορισμός της σ στο E_3. Από το Πόρισμα 4.5 έχουμε

$$Irr(a_3,\mathbb{Q})=\prod_{h\in Gal(E_3,\mathbb{Q})}(x-h(a_3))=$$
$$=(x-a_3)(x-\sigma(a_3))(x-\sigma^2(a_3))=$$
$$=(x-(\zeta+\zeta^8+\zeta^{12}+\zeta^5))(x-(\zeta^2+\zeta^3+\zeta^{11}+\zeta^{10}))(x-(\zeta^4+\zeta^6+\zeta^9+\zeta^7)).$$

Υπολογίζοντας το γινόμενο και χρησιμοποιώντας τις σχέσεις $\zeta^{13}=1$ και $\zeta^{12}+\zeta^{11}+...+1=0$ βρίσκουμε μετά από αρκετές πράξεις ότι $Irr(a_3,\mathbb{Q})=x^3+x^2-4x+1$.

Κατασκευάσιμα κανονικά n-γωνα

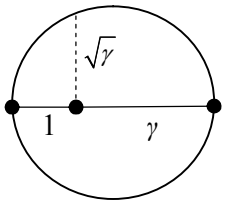
Εδώ χαρακτηρίζουμε τα κανονικά n-γωνα[4] που είναι κατασκευάσιμα με κανόνα και διαβήτη. Θα χρειαστούμε τα εξής αποτελέσματα.

i) *Αν ο πραγματικός αριθμός* a *είναι κατασκευάσιμος*[5]*, τότε ο βαθμός* $[\mathbb{Q}(a):\mathbb{Q}]$ *είναι δύναμη του 2.* Βλ. Θεώρημα 2.7.

ii) *Έστω* $\mathbb{Q}=F_k\subseteq F_{k-1}\subseteq ...\subseteq F_0\subseteq\mathbb{R}$ *διαδοχικές επεκτάσεις τέτοιες ώστε* $[F_i:F_{i+1}]=2$ *για κάθε* $i=0,...,k-1$. *Τότε κάθε στοιχείο του* F_0 *είναι κατασκευάσιμο.*

Απόδειξη: Με επαγωγή στο k. Αρκεί να δειχτεί το εξής. Έστω $\mathbb{Q}\subseteq F\subseteq K\subseteq\mathbb{R}$ τέτοια ώστε κάθε στοιχείο του F είναι κατασκευάσιμο και $[K:F]=2$. Τότε κάθε στοιχείο του K είναι κατασκευάσιμο.

Έστω $\alpha\in K-F$. Επειδή $[K:F]=2$, έχουμε $Irr(\alpha,F)=x^2+bx+c$, οπότε $a=(-b\pm\sqrt{b^2-4c})/2$. Το στοιχείο $\gamma=b^2-4c\in F$ είναι κατασκευάσιμο και άρα το $\sqrt{\gamma}$ είναι κατασκευάσιμο (βλ. σχήμα). Συνεπώς το a είναι κατασκευάσιμο.



iii) *Έστω* H *μια πεπερασμένη αβελιανή ομάδα τάξης* 2^k. *Τότε υπάρχει ακολουθία υποομάδων της* H $1=H_0\le H_1\le H_2\le ...\le H_k=H$ *με* $[H_{i+1}:H_i]=2$ *για κάθε* $i=0,...,k-1$.

Απόδειξη: Με επαγωγή στο k. Η περίπτωση $k=1$ είναι άμεση. Έστω $k>1$. Υπάρχει στοιχείο $a\in H$ τάξης 2.

Έστω $<a>$ η κυκλική υποομάδα που παράγεται από το a. Η ομάδα H είναι αβελιανή και η ομάδα $H/<a>$ είναι αβελιανή τάξης 2^{k-1}. Από επαγωγή, υπάρχει ακολουθία υποομάδων της $H/<a>$

$$1=H_0'\le H_1'\le H_2'\le ...\le H_{k-1}'=H/<a>$$

με $[H_{i+1}':H_i']=2$ για κάθε $i=0,...,k-2$. Ξέρουμε ότι κάθε υποομάδα της $H/<a>$ είναι της μορφής $\bar{H}/<a>$, όπου $<a>\le\bar{H}\le H$. Άρα η παραπάνω ακολουθία είναι της μορφής

$$1=\bar{H}_0/<a>\le\bar{H}_1/<a>\le\bar{H}_2/<a>\le ...\le\bar{H}_{k-1}/<a>=H/<a>$$

όπου $<a>=\bar{H}_0\le\bar{H}_1\le ...\le\bar{H}_{k-1}=H$. Θέτοντας $\bar{H}_{-1}=1$ έχουμε την ακολουθία υποομάδων

$$1=\bar{H}_{-1}\le\bar{H}_0\le\bar{H}_1\le ...\le\bar{H}_{k-1}=H,$$

όπου $[\bar{H}_{i+1}:\bar{H}_i]=[\bar{H}_{i+1}/<a>:\bar{H}_i/<a>]=2$ για κάθε $i=0,...,k-1$ και $[\bar{H}_0:\bar{H}_{-1}]=2$.

Θεώρημα 6.10 (Gauss-Wantzel) *Το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη αν και μόνο αν ο ακέραιος* $\varphi(n)$ *είναι δύναμη του 2.*

Απόδειξη Έστω $n>2$ και $\zeta=\zeta_n=\cos(2\pi/n)+i\sin(2\pi/n)$, οπότε $\zeta^{-1}=\cos(2\pi/n)-i\sin(2\pi/n)$ και

$$\zeta+\zeta^{-1}=2\cos(2\pi/n).$$

[4] Όταν λέμε *κανονικό n-γωνο* εννοούμε κυρτό πολύγωνο n ίσων πλευρών.

[5] Όταν λέμε ότι ο πραγματικός αριθμός α είναι *κατασκευάσιμος* εννοούμε ότι το σημείο (α,0) είναι κατασκευάσιμο (βλ. Ενότητα 2).

Είναι σαφές ότι $\mathbb{Q}(\zeta+\zeta^{-1})\subseteq\mathbb{R}$ και ότι το $\mathbb{Q}(\zeta)$ δεν περιέχεται στο $\mathbb{R}$. Άρα $[\mathbb{Q}(\zeta):\mathbb{Q}(\zeta+\zeta^{-1})]\geq 1$. Το ζ είναι ρίζα του $x^2-ax+1\in\mathbb{Q}(\zeta+\zeta^{-1})[x]$, όπου $a=\zeta+\zeta^{-1}$. Επομένως

$$[\mathbb{Q}(\zeta):\mathbb{Q}(\zeta+\zeta^{-1})]=2. \qquad (1)$$

Έχουμε την εξής κατάσταση.

$$\varphi(n)\begin{cases}\mathbb{Q}(\zeta)\\ \mid\ \}\,2\\ \mathbb{Q}(\zeta+\zeta^{-1})=\mathbb{Q}(\cos(2\pi/n))\\ \mid\\ \mathbb{Q}\end{cases}$$

$'\Rightarrow'$Έστω ότι το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη. Τότε ο πραγματικός αριθμός $\cos(2\pi/n)$ είναι κατασκευάσιμος. Άρα

$$[\mathbb{Q}(\zeta+\zeta^{-1}):\mathbb{Q}]=[\mathbb{Q}(\cos(2\pi/n)):\mathbb{Q}]=2^m$$

για κάποιο $m\geq 0$. Από την (1) παίρνουμε $[\mathbb{Q}(\zeta):\mathbb{Q}]=2^{m+1}$ και από το Θεώρημα 6.5 $\varphi(n)=2^{m+1}$.

$'\Leftarrow'$Έστω ότι το $\varphi(n)$ είναι δύναμη του 2. Λόγω της Πρότασης 6.6 το $\left|Gal(\mathbb{Q}(\zeta),\mathbb{Q})\right|$ είναι δύναμη του 2 και από αυτό που αναφέραμε πριν την απόδειξη, υπάρχουν υποομάδες H_i της $Gal(\mathbb{Q}(\zeta),\mathbb{Q})$ με

$$1=H_0\leq H_1\leq\ldots\leq H_k=Gal(\mathbb{Q}(\zeta),\mathbb{Q})$$

και $[H_{i+1}:H_i]=2$. Λαμβάνοντας σταθερά σώματα στην παραπάνω ακολουθία, το Θεώρημα 5.3 δίνει διαδοχικές επεκτάσεις

$$\mathbb{Q}=F_k\leq F_{k-1}\leq\ldots\leq F_0=\mathbb{Q}(\zeta)$$

με $[F_{i+1}:F_i]=2$. Άρα κάθε στοιχείο του $\mathbb{Q}(\zeta)$ είναι κατασκευάσιμο, ειδικά το

$$\cos(2\pi/n)=\frac{\zeta+\zeta^{-1}}{2}$$

είναι κατασκευάσιμο. Δηλαδή το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη.

Σημειώνουμε ότι στην απόδειξη $'\Rightarrow'$ του θεωρήματος δεν χρησιμοποιήσαμε το θεμελιώδες θεώρημα της θεωρίας Galois.

Παράδειγμα Το κανονικό 17-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη αφού $\varphi(17)=16=2^4$ ενώ το κανονικό 19-γωνο δεν είναι.

Πόρισμα 6.11 *Το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη αν και μόνο αν* $n=2^m p_1\ldots p_t$ *όπου οι* $p_1,\ldots,p_t$ *είναι διακεκριμένοι πρώτοι της μορφής* $p_i=2^{2^{s_i}}+1$.

Απόδειξη Έστω $n=2^m p_1^{m_1}\ldots p_t^{m_t}$ όπου p_i διακεκριμένοι πρώτοι. Τότε

$$\varphi(n)=\varphi(2^m)\varphi(p_1^{m_1})\ldots\varphi(p_t^{m_t})=2^{m-1}p_1^{m_1-1}(p_1-1)\ldots p_t^{m_t-1}(p_t-1).$$

Το δεξί μέλος είναι δύναμη του 2 αν και μόνο αν για κάθε i

$$m_i=1\ \text{ και }\ p_i=2^{n_i}+1.$$

Όμως αν ο $p_i=2^{n_i}+1$ είναι πρώτος, τότε το n_i είναι δύναμη του 2, γιατί αν $n_i=qr$ με $q>1$ περιττό, τότε $p_i=2^{n_i}+1=(2^r)^q+1=(2^r+1)((2^r)^{q-1}-(2^r)^{q-2}+\ldots-2^r+1)$, πράγμα που αντιφάσκει ότι ο p_i είναι πρώτος.

Σημείωση a) Οι πρώτοι της μορφής $2^{2^s}+1$ λέγονται **πρώτοι του Fermat**. Ο Fermat διατύπωσε την εικασία ότι κάθε αριθμός της μορφής $2^{2^s}+1$, $s=0,1,2,\ldots$, είναι πρώτος. Ο Euler έδειξε ότι για $s=5$, ο $2^{2^5}+1$ δεν είναι πρώτος. b) Ο Gauss έδειξε ότι αν το n είναι όπως στο Πόρισμα 6.11, τότε το κανονικό n-

γωνο είναι κατασκευάσιμο. Διατύπωσε την εικασία ότι ισχύει το αντίστροφο, πράγμα που έδειξε αργότερα ο Wantzel.

Ασκήσεις 6

Με G_n συμβολίζουμε την ομάδα Galois του x^n-1 πάνω από το $\mathbb{Q}$.

1. Έστω p πρώτος και R μεταθετικός δακτύλιος με μονάδα τέτοιος ώστε $pr=0$ γι κάθε $r\in R$. Δείξτε ότι $(a+b)^p=a^p+b^p$ για κάθε $a,b\in R$. Στην συνέχεια δείξτε ότι $(g(x))^p=g(x^p)$ για κάθε $\mathbb{Z}_p[x]$.
2. Έστω $n>2$, ζ μια πρωταρχική n-στη ρίζα της μονάδας και $\alpha=\zeta+\zeta^{-1}$. Βρείτε το $Irr(\zeta,\mathbb{Q}(\alpha))$ και την ομάδα $Gal(\mathbb{Q}(\zeta),\mathbb{Q}(\alpha))$. Ποιος είναι ο βαθμός $[\mathbb{Q}(a):\mathbb{Q}]$;
3. Υπολογίστε το $\Phi_{12}(x)$ και το $\Phi_{25}(x)$.
4. Δείξτε ότι
   a. $\Phi_{p^2}(x)=\Phi_p(x^p)$ για κάθε πρώτο p
   b. $\Phi_{2n}(x)=\Phi_n(-x)$ για κάθε περιττό $n>1$.
5. Έστω m,n θετικοί ακέραιοι με $\mu\kappa\delta(m,n)=1$. Δείξτε τα εξής.
   a. $G_{mn}\simeq G_m\times G_n$.
   b. $\mathbb{Q}(\zeta_m,\zeta_n)=\mathbb{Q}(\zeta_{mn})$.
   c. $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$.
   d. Διατυπώστε και αποδείξτε μια γενίκευση των b,c που ισχύει χωρίς την υπόθεση $\mu\kappa\delta(m,n)=1$.
6. Ποιες από τις επόμενες ομάδες είναι κυκλικές; Αν μια ομάδα είναι κυκλική, να βρεθεί ένας γεννήτορας. Για κάθε ομάδα βρείτε την αντιστοιχία Galois.
   a. G_8.
   b. G_{10}.
7. Δείξτε τα εξής.
   a. $\prod_{k=0}^{4}(x-2\cos(2^{2k+1}\pi/11))=x^5+x^4-4x^3-3x^2+3x+1$. (Βλ. Παράδειγμα 6.8).
   b. Έστω $\zeta=\zeta_{11}$. Τότε το μοναδικό υπόσωμα του $\mathbb{Q}(\zeta)$ βαθμού 2 πάνω από το $\mathbb{Q}$ είναι το $\mathbb{Q}(a)$, όπου $a=\zeta+\zeta^3+\zeta^4+\zeta^5+\zeta^9$.
8.
   a. Υπολογίστε το $\Phi_{14}(x)$.
   b. Δείξτε ότι $\cos(2\pi/7)+\cos(8\pi/7)+\cos(10\pi/7)=-1/2$.
   c. Αληθεύει ότι $G_{14}\simeq G_7$;
9. Δείξτε ότι $\sqrt[3]{2}\notin\mathbb{Q}(\zeta_n)$ για κάθε n.
10. Έστω $\zeta=\zeta_7$ και $a=\zeta+\zeta^2+\zeta^4$. Τότε $\mathbb{Q}(a)=\mathbb{Q}(i\sqrt{7})$.
11. Δείξτε ότι $G_{15}\simeq\mathbb{Z}_2\times\mathbb{Z}_4$ και βρείτε το $Irr(a,\mathbb{Q})$, όπου $a=2\cos(2\pi/15)$.
12. Έστω $a\in\mathbb{R}$ τέτοιο ώστε $\deg Irr(a,\mathbb{Q})$ είναι δύναμη του 2. Αληθεύει ότι το a είναι κατασκευάσιμο;
13. Έστω $p>2$ πρώτος, $K\subseteq\mathbb{C}$ το σώμα ριζών του x^p-2 πάνω από το $\mathbb{Q}$ και $G=Gal(K,\mathbb{Q})$. Είδαμε στην άσκηση 4.6 ότι $|G|=p(p-1)$. Δείξτε τα εξής.
    a. Η ομάδα G δεν είναι αβελιανή.
    b. Για κάθε διαιρέτη d του $p-1$ η G έχει κανονική υποομάδα δείκτη d.
14. Αν το κανονικό n-γωνο και το κανονικό m-γωνο είναι κατασκευάσιμα με κανόνα και διαβήτη, τότε το κανονικό e-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη όπου $e=\varepsilon\kappa\pi(m,n)$.

15.
   a. Θεωρώντας το ζ_{29} δείξτε ότι υπάρχει $f(x) \in \mathbb{Q}[x]$ βαθμού 7 με ομάδα Galois τάξης 7.
   b. *Για κάθε πρώτο p υπάρχει υπάρχει $f(x) \in \mathbb{Q}[x]$ βαθμού p με ομάδα Galois τάξης p.
16. Έστω $\mathbb{Q} \subseteq K$ πεπεπρασμένη επέκταση του $\mathbb{Q}$ με $K \subseteq \mathbb{C}$. Το πλήθος των πρωταρχικών n-στων ριζών ριζών της μονάδας, καθώς το n διατρέχει τους θετικούς ακέραιους, που περιέχονται στο K είναι πεπερασμένο.
17. Στο τέλος του μνημειώδους έργου *Disquisitiones Arithmeticae*, ο Gauss καταγράφει την ακολουθία 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.
    Ποια είναι η ακολουθία αυτή;
18. Εξετάστε ποιες από τις ακόλουθες προτάσεις είναι αληθείς.
   a. Κάθε υπόσωμα του $\mathbb{Q}(\zeta_n)$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$.
   b. Αν $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\zeta_n)$ είναι διαδοχικές επεκτάσεις, τότε $\left|Gal(E,\mathbb{Q})\right| = [E:\mathbb{Q}]$.
   c. Αν $\mathbb{Q} \subseteq E$ είναι πεπερασμένη επέκταση, τότε $\left|Gal(E,\mathbb{Q})\right| = [E:\mathbb{Q}]$.
   d. Υπάρχει n τέτοιο ώστε $Gal(\mathbb{Q}(\zeta_n),E) \simeq S_3$ για κάποιο E.
   e. Για κάθε $n > 2$, $\deg Irr(\cos(2\pi/n) = \varphi(n)/2$.

7. Επιλύσιμες ομάδες

Βασικά σημεία

- Για κάθε $n \geq 5$ η ομάδα S_n δεν είναι επιλύσιμη.
- Υποομάδα και ομομορφική εικόνα επιλύσιμης ομάδας είναι επιλύσιμη.

Από τις επιλύσιμες ομάδες θα αναφερθούμε μόνο σε εκείνα τα αποτελέσματα που θα χρειαστούμε στην Ενότητα 8.

Ορισμός 7.1 *Μια ομάδα G λέγεται* ***επιλύσιμη*** *αν υπάρχει πεπερασμένη ακολουθία υποομάδων*

$$1 = G_m \leq G_{m-1} \leq \ldots \leq G_1 \leq G_0 = G$$

τέτοια ώστε για κάθε $i = 1, \ldots, m$

- *η G_i είναι κανονική στη G_{i-1} και*
- *η ομάδα G_{i-1}/G_i είναι αβελιανή.*

Υπενθυμίζουμε το εξής.

Λήμμα 7.2

i) Έστω G ομάδα και H κανονική υποομάδα της G. Τότε η ομάδα πηλίκο G/H είναι αβελιανή αν και μόνο αν $aba^{-1}b^{-1} \in H$ για κάθε $a, b \in G$.

ii) Έστω κύκλος $(i_1 i_2 \ldots i_t) \in S_n$ και $\sigma \in S_n$. Τότε $\sigma(i_1 i_2 \ldots i_t)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_t))$.

Απόδειξη i) Ισχύει $abH = baH \Leftrightarrow (ba)^{-1}(ab) \in H \Leftrightarrow a^{-1}b^{-1}ab \in H$. Παρατηρούμε ότι $a^{-1}b^{-1}ab \in H$ για κάθε $a, b \in G$ αν και μόνο αν $aba^{-1}b^{-1} \in H$ για κάθε $a, b \in G$.

ii) Υπολογίζουμε τη μετάθεση $\sigma(i_1 i_2 \ldots i_t)\sigma^{-1}$. Έχουμε

$$\sigma(i_1 i_2 \ldots i_t)\sigma^{-1}(\sigma(i_k)) = \sigma(i_1 i_2 \ldots i_t)(i_k) = \sigma(i_{k+1}),\ k = 1, \ldots, t-1,$$
$$\sigma(i_1 i_2 \ldots i_t)\sigma^{-1}(\sigma(i_t)) = \sigma(i_1 i_2 \ldots i_t)(i_t) = \sigma(i_1),$$
$$\sigma(i_1 i_2 \ldots i_t)\sigma^{-1}(\sigma(j)) = \sigma(i_1 i_2 \ldots i_t)(j) = \sigma(j),\ j \in \{1, \ldots, n\} - \{i_1, \ldots, i_t\}.$$

Άρα $\sigma(i_1 i_2 \ldots i_t)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_t))$.

Παραδείγματα 7.3

i) Κάθε αβελιανή ομάδα G είναι επιλύσιμη καθώς έχουμε την ακολουθία $1 \leq G$.

ii) Η S_3 είναι επιλύσιμη αφού έχουμε την ακολουθία υποομάδων

$$1 \leq A_3 \leq S_3$$

και ξέρουμε ότι η A_3 είναι κανονική στη S_3, ότι η S_3/A_3 είναι αβελιανή (έχει τάξη 2) και ότι η A_3 είναι αβελιανή (έχει τάξη 3).

iii) Η S_4 είναι επιλύσιμη. Πράγματι, έστω $H = \{1, (12)(34), (13)(24), (14)(23)\}$. Είναι σαφές ότι κάθε στοιχείο της H είναι άρτια μετάθεση και άρα $H \subseteq A_4$. Εύκολα αποδεικνύεται ότι το H είναι κλειστό σύνολο ως προς την πράξη της S_4 και άρα είναι υποομάδα της A_4. Επίσης εύκολα αποδεικνύεται ότι η H είναι αβελιανή. Η H είναι κανονική στην A_4 καθώς για κάθε $\sigma \in A_4$ και κάθε $(ij)(kl) \in H$ έχουμε σύμφωνα με το Λήμμα 7.2 ii)

$$\sigma(ij)(kl)\sigma^{-1} = (\sigma(ij)\sigma^{-1})(\sigma(kl)\sigma^{-1}) = (\sigma(i)\sigma(j))(\sigma(k)\sigma(l)) \in H.$$

Η ομάδα A_4/H είναι αβελιανή γιατί έχει τάξη $12/4 = 3$.

Ξέρουμε ότι η A_4 είναι κανονική στη S_4 και ότι η S_4/A_4 είναι αβελιανή γιατί έχει τάξη 2.

Από τα παραπάνω έπεται ότι η ακολουθία υποομάδων

$$1 \le H \le A_4 \le S_4$$

πληροί τις ιδιότητες του Ορισμού 7.1 και η S_4 είναι επιλύσιμη.

iv) Η διεδρική ομάδα D_4 (των συμμετριών του τετραγώνου) είναι επιλύσιμη. Αφήνουμε ως άσκηση την επαλήθευση ότι η ακολουθία $1 \le H \le D_4$ πληροί τις ιδιότητες του Ορισμού 7.1, όπου H είναι η υποομάδα των στροφών.

Θεώρημα 7.4 *Για κάθε $n \ge 5$, η ομάδα S_n δεν είναι επιλύσιμη.*

Απόδειξη Έστω $n \ge 5$. Υποθέτουμε ότι υπάρχει ακολουθία υποομάδων

$$1 = G_m \le G_{m-1} \le ... \le G_1 \le G_0 = S_n$$

με τις ιδιότητες του Ορισμού 7.1. Έστω $(ijk) \in S_n$ ένας κύκλος μήκος 3 και $a, b \in \{1,2,...,n\} - \{i, j, k\}$ με $a \ne b$. (Υπάρχουν τέτοια a, b αφού $n \ge 5$). Επειδή η ομάδα S_n / G_1 είναι αβελιανή, από το Λήμμα 7.2 i) έχουμε

$$(ajk)(bji)(ajk)^{-1}(bji)^{-1} \in G_1.$$

Αλλά

$$(ajk)(bji)(ajk)^{-1}(bji)^{-1} = (ajk)(bji)(kja)(ijb) = (ijk).$$

Δηλαδή η G_1 περιέχει όλους τους κύκλους μήκους 3.

Επαναλαμβάνοντας το ίδιο επιχείρημα για G_1/G_2 στη θέση της S_n/G_1 παίρνουμε ότι η G_2 περιέχει όλους τους κύκλους μήκους 3. Συνεχίζοντας έτσι φτάνουμε στο συμπέρασμα ότι η $G_m = 1$ περιέχει όλους τους κύκλους μήκους 3, άτοπο.

Πρόταση 7.5 *Έστω G επιλύσιμη ομάδα.*

i) Αν $f : G \to G'$ είναι επιμορφισμός ομάδων, τότε η G' είναι επιλύσιμη.

ii) Αν $H \le G$, τότε η H είναι επιλύσιμη.

Απόδειξη Έστω

$$1 = G_m \le G_{m-1} \le ... \le G_1 \le G_0 = G$$

μια ακολουθία υποομάδων της G με τις ιδιότητες του Ορισμού 7.1.

i) Έχουμε την ακολουθία

$$1 = f(G_m) \le f(G_{m-1}) \le ... \le f(G_1) \le f(G_0) = G'$$

υποομάδων της G'. Επειδή η G_i είναι κανονική στη G_{i-1}, η $f(G_i)$ είναι κανονική στη $f(G_{i-1})$ αφού $f(a)f(b)f(a)^{-1} = f(aba^{-1}) \in f(G_{i-1})$ για κάθε $a \in G_{i-1}$, $b \in G_i$.

Η απεικόνιση $G_{i-1} \to f(G_{i-1})/f(G_i)$, $g \mapsto f(g)f(G_i)$, είναι επιμορφισμός ομάδων και ο πυρήνας της περιέχει το G_i. Συνεπώς υπάρχει επιμορφισμός ομάδων $G_{i-1}/G_i \to f(G_{i-1})/f(G_i)$. Επειδή η G_{i-1}/G_i είναι αβελιανή, η $f(G_{i-1})/f(G_i)$ είναι αβελιανή. Άρα η G' είναι επιλύσιμη ομάδα.

ii) Έχουμε την ακολουθία

$$1 = H \cap G_m \le H \cap G_{m-1} \le ... \le H \cap G_1 \le H \cap G_0 = H$$

υποομάδων της H.

Η απεικόνιση $H \cap G_{i-1} \to G_{i-1}/G_i$, $g \mapsto gG_i$, είναι ομομορφισμός ομάδων και ο πυρήνας της είναι η $H \cap G_i$. Άρα η $H \cap G_i$ είναι κανονική στην $H \cap G_{i-1}$ και υπάρχει μονομορφισμός ομάδων $H \cap G_{i-1}/H \cap G_i \to G_{i-1}/G_i$. Επειδή η G_{i-1}/G_i είναι αβελιανή έπεται ότι η $H \cap G_{i-1}/H \cap G_i$ είναι αβελιανή. Άρα η H είναι επιλύσιμη ομάδα.

Για παράδειγμα, κάθε υποομάδα της S_4 είναι επιλύσιμη ομάδα.

Ασκήσεις 7

1. Έστω $F \subseteq E \subseteq K$, όπου K σώμα ριζών πάνω από το F και το F έχει χαρακτηριστική 0. Αν το E είναι σώμα ριζών πάνω από το F και η ομάδα $Gal(K,F)$ είναι επιλύσιμη, τότε η ομάδα $Gal(E,F)$ είναι επιλύσιμη.
2. Δείξτε τον ισχυρισμό στο Παράδειγμα 7.3 iv).
3. Δείξτε ότι η ομάδα Galois ανάγωγου πολυωνύμου πάνω από το $\mathbb{Q}$ βαθμού 2, 3 ή 4 είναι επιλύσιμη.
4. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.
   a. Η ομάδα A_4 είναι επιλύσιμη.
   b. Η ομάδα A_5 είναι επιλύσιμη.
   c. Η ομάδα G είναι επιλύσιμη αν και μόνο αν η $S_4 \times G$ είναι επιλύσιμη.
5. Έστω k σώμα. Δείξτε ότι η ομάδα $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(k) \,|\, ac \neq 0\}$ με πράξη τον πολλαπλασιασμό πινάκων είναι επιλύσιμη.

8. Πολυώνυμα επιλύσιμα με ριζικά

Βασικά σημεία

- Επέκταση με ριζικά και πολυώνυμο επιλύσιμο με ριζικά.
- Θεώρημα του Galois.
- Παράδειγμα πολυωνύμου που δεν είναι επιλύσιμο με ριζικά.

Όλα τα σώματα που θεωρούμε εδώ είναι υποσώματα του $\mathbb{C}$. Αν F σώμα και $f(x) \in F[x]$, η ομάδα Galois του $f(x)$ πάνω από το F είναι η $Gal(K,F)$, όπου K το σώμα ριζών του $f(x)$ πάνω από το F.

Ορισμός 8.1 *Μια επέκταση K του F λέγεται **επέκταση με ριζικά** (ή **ριζική επέκταση**) αν υπάρχει πεπερασμένη ακολουθία επεκτάσεων*

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_t = K$$

τέτοια ώστε για κάθε $i = 1,..,t$ υπάρχει $a_i \in F_i$ και θετικός ακέραιος n_i με

- $F_i = F_{i-1}(a_i)$ *και*
- $a_i^{n_i} \in F_{i-1}$.

*Ένα πολυώνυμο $f(x) \in F[x]$ λέγεται **επιλύσιμο με ριζικά** πάνω από το F αν υπάρχει επέκταση με ριζικά K του F που περιέχει το σώμα ριζών του $f(x)$ πάνω από το F.*

Παραδείγματα

i) Το $\mathbb{Q}(\sqrt{3}, \sqrt[5]{7+\sqrt{2}})$ είναι επέκταση με ριζικά του $\mathbb{Q}$ αφού έχουμε την ακολουθία
$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt[5]{7+\sqrt{2}})$ και $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt[5]{7+\sqrt{2}}) = \mathbb{Q}(\sqrt{3},\sqrt[5]{7+\sqrt{2}})$.

ii) Το $x^2 + ax + b \in \mathbb{Q}$ είναι επιλύσιμο με ριζικά αφού οι ρίζες του $\dfrac{-a \pm \sqrt{a^2-4b}}{2}$ ανήκουν στο $\mathbb{Q}(\sqrt{a^2-4b})$, που είναι επέκταση με ριζικά του $\mathbb{Q}$. (Εδώ το $\sqrt{a^2-4b}$ συμβολίζει μια μιγαδική τετραγωνική ρίζα του a^2-4b).

iii) Έστω $a,b \in \mathbb{R}$, όπου $a = \sqrt[3]{-1+\sqrt{2}}$, $b = \sqrt[3]{-1-\sqrt{2}}$, και $\omega \in \mathbb{C} - \mathbb{R}$ με $\omega^3 = 1$. Οι ρίζες του $f(x) = x^3 + 3x + 2$, είναι οι

$$a+b,$$
$$\omega a + \omega^2 b,$$
$$\omega^2 a + \omega b.$$

Το $f(x)$ είναι επιλύσιμο με ριζικά πάνω από το $\mathbb{Q}$ γιατί το $\mathbb{Q}(\omega,a,b)$ είναι επέκταση με ριζικά του $\mathbb{Q}$ καθώς έχουμε την ακολουθία

$$\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}(\omega,\sqrt{2}) \subseteq \mathbb{Q}(\omega,\sqrt{2},a) \subseteq \mathbb{Q}(\omega,\sqrt{2},a,b).$$

Θεώρημα 8.2 (Galois) *Αν το $f(x) \in F[x]$ είναι επιλύσιμο με ριζικά, τότε η ομάδα Galois του $f(x)$ πάνω από το F είναι επιλύσιμη.*

Για την απόδειξη χρειαζόμαστε δύο αποτελέσματα. Το πρώτο είναι ιδιαίτερα απλό.

Λήμμα 8.3 *Έστω F σώμα που περιέχει πρωταρχική n-στη ρίζα της μονάδας και έστω $a \in \mathbb{C}$ με $a^n \in F$. Τότε η ομάδα $Gal(F(a),F)$ είναι αβελιανή.*

Απόδειξη Έστω $\sigma,\tau \in Gal(F(a),F)$, $\zeta \in F$ μια πρωταρχική n-στη ρίζα της μονάδας και $a^n = b \in F$. Τότε $\sigma(a)^n = \sigma(b) = b$, οπότε $\sigma(a) = \zeta^{k_\sigma} a$ για κάποιο ακέραιο k_σ. Άρα

$$\tau\sigma(a) = \tau(\zeta^{k_\sigma} a) = \zeta^{k_\sigma}\tau(a) = \zeta^{k_\sigma}\zeta^{k_\tau} a = \zeta^{k_\sigma + k_\tau} a$$

και όμοια $\sigma\tau(a) = \zeta^{k_\tau + k_\sigma} a$. Άρα $\tau\sigma = \sigma\tau$.

Παράδειγμα Έστω $K = \mathbb{Q}(\zeta_n, \sqrt[n]{2})$ και $G = Gal(K, \mathbb{Q})$. Η G είναι επιλύσιμη. Πράγματι, έχουμε την ακολουθία

$$1 \le Gal(K, \mathbb{Q}(\zeta_n) \le G$$

και παρατηρούμε τα εξής.

- Η ομάδα $Gal(K, \mathbb{Q}(\zeta_n)$ είναι αβελιανή από το Λήμμα 8.3.
- Επειδή το $\mathbb{Q}(\zeta_n)$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$, από το Θεώρημα 5.3 έπεται ότι η υποομάδα $Gal(K, \mathbb{Q}(\zeta_n)$ είναι κανονική στη G και $G/Gal(K, \mathbb{Q}(\zeta_n)) \simeq Gal(\mathbb{Q}(\zeta_n), \mathbb{Q})$. Η τελευταία ομάδα είναι αβελιανή από την Πρόταση 6.6.

Για να αποδείξουμε το Θεώρημα 8.2 θέλουμε να εφαρμόσουμε το θεμελιώδες θεώρημα της θεωρίας Galois. Όμως το K δεν είναι αναγκαστικά σώμα ριζών πάνω από το F. Για παράδειγμα η επέκταση $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ είναι επέκταση με ριζικά αλλά το $\mathbb{Q}(\sqrt[3]{2})$ δεν είναι σώμα ριζών πάνω από το $\mathbb{Q}$. Το επόμενο λήμμα μας επιτρέπει να παρακάμψουμε το εμπόδιο αυτό.

Λήμμα 8.4 *Έστω K μια επέκταση με ριζικά του F. Τότε υπάρχει επέκταση L του K που είναι σώμα ριζών πάνω από το F και επέκταση με ριζικά του F.*

Απόδειξη Έχουμε $K = F(a_1, ..., a_t)$ και $a_i^{n_i} \in F(a_1, ..., a_{i-1})$ για κάθε $i = 1, ..., t$. (Για $i = 1$ εννοούμε ότι $a_1^{n_1} \in F$). Έστω L το σώμα ριζών του

$$\prod_i Irr(a_i, F)$$

πάνω από το F. Αρκεί να δείξουμε ότι το L είναι επέκταση με ριζικά του K.

Έστω $a_i = a_{i1}, a_{i2}, ..., a_{im_i}$ οι ρίζες του $Irr(a_i, F)$. Για κάθε a_{ij}, υπάρχει $\sigma \in Gal(L, F)$ με $a_{ij} = \sigma(a_i)$ σύμφωνα με το Πόρισμα 3.11. Τότε $a_{ij}^{n_i} = \sigma(a_i^{n_i})$. Αλλά $a_i^{n_i} \in F(a_1, ..., a_{i-1})$. Επομένως

$$a_{ij}^{n_i} = \sigma(a_i^{n_i}) \in F(\sigma(a_1), ..., \sigma(a_{i-1})) \subseteq F(a_{11}, ..., a_{1m_1}, ..., a_{i-11}, ..., a_{i-1m_{i-1}})$$

γιατί $\sigma(a_j) \in \{a_{j1}, ..., a_{jm_j}\}$. Συνεπώς ξεκινώντας με το σώμα $K = F(a_1, a_2 ..., a_t)$ και επισυνάπτοντας κάθε φορά ένα από τα στοιχεία

$$a_{12}, a_{13}, ..., a_{1m_1},$$
$$a_{22}, a_{23}, ..., a_{2m_2},$$
$$\vdots$$
$$a_{t2}, a_{t3}, ..., a_{tm_t},$$

με την αναγραφόμενη σειρά, παίρνουμε μια επέκταση που είναι επέκταση με ριζικά

$$F(a_1, a_2 ..., a_t) \subseteq F(a_1, a_{12}, a_2 ..., a_t) \subseteq ... \subseteq F(a_1, a_{12}, ..., a_{1m_1}, a_2, ..., a_t) \subseteq$$
$$F(a_1, a_{12}, ..., a_{1m_1}, a_2, a_{21}, ..., a_t) \subseteq ... \subseteq F(a_1, a_{12}, ..., a_{1m_1}, a_2, a_{22}, ..., a_{2m_2}, a_3, ..., a_t) \subseteq ...$$
$$\subseteq F(a_1, a_{12}, ..., a_{1m_1}, a_2, a_{22}, ..., a_{2m_2}, a_3, a_{32}, ..., a_{3m_3}, ..., a_t, a_{t2}, ..., a_{tm_t}).$$

Παράδειγμα Με το συμβολισμό της απόδειξης του Λήμματος 8.4, αν $F = \mathbb{Q}$, $K = \mathbb{Q}(a_1, a_2)$ και $a_1 = \sqrt[3]{2}$, $a_2 = \sqrt[5]{1 + \sqrt[3]{2}}$, τότε $L = \mathbb{Q}(a_1, \zeta_3 a_1, \zeta_3^{\,2} a_1, a_2, \zeta_5 a_2, \zeta_5^{\,2} a_2, \zeta_5^{\,3} a_2, \zeta_5^{\,4} a_2)$. Αφήνουμε την απόδειξη σαν άσκηση. Παρατηρούμε ότι $L = K(\zeta_3, \zeta_5)$.

Σημείωση Το L της απόδειξης του Λήμματος 8.4 συνήθως λέγεται η **κανονική θήκη** του K στο $\mathbb{C}$ πάνω από το F. Είναι το μικρότερο υπόσωμα του $\mathbb{C}$ που περιέχει το K και είναι σώμα ριζών πάνω από το F.

Απόδειξη του Θεωρήματος 8.2: Από την υπόθεση υπάρχει πεπερασμένη ακολουθία επεκτάσεων

$$F = F_0 \subseteq F_1 \subseteq \ldots F_{t-1} \subseteq F_t = K \tag{1}$$

τέτοια ώστε το K περιέχει το σώμα ριζών E του $f(x)$ πάνω από το F και για κάθε $i = 1,..,t$ υπάρχει $a_i \in F_i$ και θετικός ακέραιος n_i με

- $F_i = F_{i-1}(a_i)$ και
- $a_i^{n_i} \in F_{i-1}$.

Από το Λήμμα 8.4 μπορούμε να υποθέσουμε ότι το K είναι σώμα ριζών πάνω από το F.

Έστω $n = n_1 n_2 \ldots n_t$ και ζ μια πρωταρχική n-στη ρίζα του n. Από την (1) παίρνουμε επισυνάπτοντας το ζ την ακολουθία επεκτάσεων

$$\begin{array}{ccccccccc} F & \subseteq & F_0(\zeta) & \subseteq & F_1(\zeta) & \subseteq & \ldots & \subseteq & F_t(\zeta) = K(\zeta) \\ \| & & \| & & \| & & & & \| \\ F & \subseteq & E_0 & \subseteq & E_1 & \subseteq & \ldots & \subseteq & E_t = L \end{array} \tag{2}$$

και θέτουμε $L = K(\zeta), E_i = F_i(\zeta)$, $i = 0,\ldots,t$.

Από την (2) παίρνουμε την ακολουθία υποομάδων της $Gal(L,F)$,

$$Gal(L,F) \supseteq Gal(L,E_0) \supseteq Gal(L,E_1) \supseteq \ldots \supseteq Gal(L,E_{t-1}) \supseteq Gal(L,E_t) = Gal(L,L) = 1. \tag{3}$$

Θα δείξουμε ότι η $Gal(L,F)$ είναι επιλύσιμη.

Αν $p(x) \in F[x]$ είναι τέτοιο που το K είναι σώμα ριζών του $p(x)$ πάνω από το F, τότε το $L = K(\zeta)$ είναι σώμα ριζών του $(x^n - 1)p(x)$ πάνω από το F. Επίσης, το E_i είναι σώμα ριζών του $x^{n_i} - a_i^{n_i}$ πάνω από το E_{i-1} γιατί $E_i = E_{i-1}(a_i)$, $a_i^{n_i} \in E_{i-1}$ και το E_i περιέχει πρωταρχική n_i στη ρίζα της μονάδας, για παράδειγμα τη ζ^{n/n_i}.

Δηλαδή στην ακολουθία (2) κάθε διαδοχική επέκταση είναι σώμα ριζών και επιπλέον το L είναι σώμα ριζών πάνω από το F και πάνω από κάθε E_i. Εφαρμόζοντας το θεμελιώδες θεώρημα της θεωρίας Galois στην ακολουθία

$$E_{i-1} \subseteq E_i \subseteq L$$

παίρνουμε ότι η $Gal(L,E_i)$ είναι κανονική στη $Gal(L,E_{i-1})$ και

$$Gal(L,E_{i-1}) / Gal(L,E_i) \simeq Gal(E_i,E_{i-1}).$$

Από το Λήμμα 8.3, κάθε ομάδα $Gal(E_i,E_{i-1})$ είναι αβελιανή.

Επίσης, η $Gal(L,E_0)$ είναι κανονική στη $Gal(L,F)$, γιατί το $E_0 = F(\zeta)$ είναι σώμα ριζών πάνω από το F, και

$$Gal(L,F) / Gal(L,E_0) \simeq Gal(E_0,F).$$

Η ομάδα $Gal(E_0,F)$ είναι αβελιανή από την Πρόταση 6.6. Από τα προηγούμενα και τη (3) έπεται ότι η $Gal(L,F)$ είναι επιλύσιμη σύμφωνα με τον Ορισμό 7.1.

Τώρα θα δείξουμε ότι η $Gal(E,F)$ είναι επιλύσιμη.

Έχουμε

$$F \subseteq E \subseteq L.$$

Επειδή το E είναι σώμα ριζών πάνω από το F, από το θεμελιώδες θεώρημα της θεωρίας Galois παίρνουμε ότι ομάδα $Gal(L,E)$ είναι κανονική στη $Gal(L,F)$ και

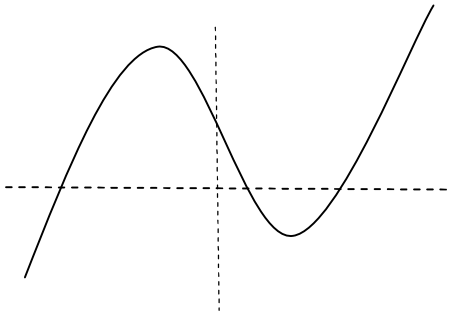
$$Gal(L,F) / Gal(L,E) \simeq Gal(E,F).$$

Επειδή η $Gal(L,F)$ είναι επιλύσιμη, από την Πρόταση 7.5 ii) έπεται ότι η $Gal(E,F)$ είναι επιλύσιμη.

Παράδειγμα 8.5 Το πολυώνυμο $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ δεν είναι επιλύσιμο με ριζικά.

Θα δείξουμε ότι η ομάδα Galois του $f(x)$ είναι ισόμορφη με την ομάδα S_5 που, όπως είδαμε στο Θεώρημα 7.4, δεν είναι επιλύσιμη. Τότε από το Θεώρημα 8.4, το $f(x)$ δεν είναι επιλύσιμο με ριζικά.

Η παράγωγος του $f(x)$ είναι $10x^4 - 10$ και εύκολα επαληθεύεται η $f(x)$ έχει ακριβώς ένα τοπικό μέγιστο και ακριβώς ένα τοπικό ελάχιστο (στα $x = -1$ και $x = 1$ αντίστοιχα). Έχουμε $f(-1) > 0$ και $f(1) < 0$. Συνεπώς η $f(x)$ έχει ακριβώς 3 πραγματικές ρίζες.



Το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ σύμφωνα με το κριτήριο του Eisenstein. Έστω K το σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$ και $a \in K$ ρίζα του $f(x)$. Τότε

$$\left|Gal(K,\mathbb{Q})\right| = [K:\mathbb{Q}] = [K:\mathbb{Q}(a)][\mathbb{Q}(a):\mathbb{Q}]$$

σύμφωνα με το Θεώρημα 4.6 και το Θεώρημα 1.10. Ισχύει $[\mathbb{Q}(a):\mathbb{Q}] = \deg f(x) = 5$ από την Πρόταση 1.8. Συνεπώς το 5 διαιρεί την τάξη της $Gal(K,\mathbb{Q})$. Επειδή η $Gal(K,\mathbb{Q})$ είναι υποομάδα της S_5 συμπεραίνουμε ότι η $Gal(K,\mathbb{Q})$ περιέχει κύκλο μήκους 5.

Από την άλλη μεριά η $Gal(K,\mathbb{Q})$ περιέχει κύκλο μήκους 2 γιατί ο περιορισμός στο K της απεικόνισης $\mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$, όπου $\overline{z}$ ο συζυγής του z, είναι ισομορφισμός $K \to K$ που σταθεροποιεί τις τρεις πραγματικές ρίζες και αντιμεταθέτει τις δύο μη πραγματικές ρίζες.

Σύμφωνα με το επόμενο λήμμα, έχουμε $Gal(K,\mathbb{Q}) = S_5$.

Λήμμα 8.6 *Αν μια υποομάδα H της S_5 περιέχει κύκλο μήκους 5 και κύκλο μήκους 2 τότε $H = S_5$.*

Απόδειξη Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\tau = (12) \in H$ και, αντικαθιστώντας τον κύκλο μήκους 5 με κατάλληλη δύναμή του, ότι $\sigma = (12abc) \in H$. Έχουμε

$$\sigma^k \tau \sigma^{-k} \in H$$

για κάθε k. Χρησιμοποιώντας το Λήμμα 7.2 έχουμε για $k = 0,1,2,3,4$ αντίστοιχα ότι

$$(12), (2a), (ab), (bc), (c1) \in H.$$

Όμοια, τα δεξιά μέλη των παρακάτω σχέσεων ανήκουν στο H.

$$(12)(2a)(12) = (1a),$$
$$(ab)(1a)(ab) = (1b),$$
$$(12)(1b)(12) = (2b),$$
$$(2b)(bc)(2b) = (2c),$$
$$(2a)(2c)(2a) = (ac).$$

Τελικά η H περιέχει όλους τους κύκλους μήκους 2 και άρα $H = S_5$, αφού κάθε μετάθεση είναι γινόμενο κύκλων μήκους 2.

Σημείωση Επισημαίνουμε ότι ισχύει το αντίστροφο του θεωρήματος 8.2.

Ασκήσεις 8

1. Να βρεθεί μια επέκταση με ριζικά του $\mathbb{Q}$ που περιέχει το $\dfrac{\sqrt[3]{3-\sqrt{2}}}{4+\sqrt{2}}$.
2. Δείξτε ότι η ομάδα Galois του x^6-4x^3+1 είναι επιλύσιμη.
3. Δείξτε ότι το $x^5-10x-5$ δεν είναι επιλύσιμο με ριζικά.
4. Αληθεύει ότι το x^6-4x^3+4 είναι επιλύσιμο με ριζικά;
5. Δείξτε τα εξής.
   a. Η ομάδα Galois του $(x^m-2)(x^n-3)$ είναι επιλύσιμη για κάθε θετικούς ακέραιους m,n.
   b. Η ομάδα $Gal(K,\mathbb{Q})$ είναι επιλύσιμη, όπου $K=\mathbb{Q}(\zeta_3,\zeta_{10},\sqrt[3]{2})$.
6. Έστω $f(x)\in\mathbb{Q}[x]$ ανάγωγο. Αν το $f(x)$ έχει μία ρίζα σε επέκταση με ριζικά, τότε είναι επιλύσιμο με ριζικά.
7. Έστω p πρώτος.
   a. Δείξτε την εξής γενίκευση του Λήμματος 8.6. Αν μια υποομάδα H της S_p περιέχει κύκλο μήκους p και κύκλο μήκους 2 τότε $H=S_p$.
   b. Αν το ανάγωγο $f(x)\in\mathbb{Q}[x]$ έχει βαθμό p, όπου $p\geq 5$, και ακριβώς δύο μη πραγματικές ρίζες, τότε δεν είναι επιλύσιμο με ριζικά.
   c. Το $x^p-2px+p$ έχει ομάδα Galois τη S_p και άρα δεν είναι επιλύσιμο με ριζικά αν $p\geq 5$.
8. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.
   a. Κάθε επέκταση με ριζικά είναι πεπερασμένη.
   b. Κάθε πεπερασμένη επέκταση του $\mathbb{Q}$ είναι επέκταση με ριζικά.
   c. Το $\mathbb{Q}(\sqrt[5]{2})$ είναι επέκταση του $\mathbb{Q}$ με ριζικά και όχι σώμα ριζών πάνω από το $\mathbb{Q}$.
   d. Το $\mathbb{Q}(\sqrt[5]{2},\zeta_5)$ είναι επέκταση του $\mathbb{Q}$ με ριζικά και σώμα ριζών πάνω από το $\mathbb{Q}$.

9. Πεπερασμένα σώματα

Βασικά σημεία

- Ύπαρξη και μοναδικότητα πεπερασμένου σώματος.
- Διάγραμμα υποσωμάτων πεπερασμένου σώματος.
- Η πολλαπλασιαστκή ομάδα πεπερασμένου σώματος είναι κυκλική ομάδα.
- Ομάδα Galois πεπερασμένου σώματος.
- Ανάλυση του $x^{p^n} - x$.

Ιδιότητες, ύπαρξη και μοναδικότητα

Έστω K πεπερασμένο σώμα και E υπόσωμα του K. Τότε το K είναι E-διανυσματικός χώρος. Επειδή ο διανυσματικός χώρος K είναι πεπερασμένα παραγόμενος (ως πεπερασμένο σύνολο), υπάρχει πεπερασμένη βάση $\{u_1,...,u_n\}$ του K. Συνεπώς κάθε στοιχείο του K γράφεται μοναδικά στη μορφή $a_1u_1 + a_2u_n + ... + a_nu_n$, όπου $a_i \in E$. Άρα $|K| = |E|^n$. Θεωρώντας την ειδική περίπτωση $E = \mathbb{Z}_p$, όπου p είναι η χαρακτηριστική του K, παίρνουμε $|K| = p^n$. Δηλαδή, το πλήθος των στοιχείων πεπερασμένου σώματος είναι δύναμη πρώτου.

Πρόταση 9.1 *Έστω K πεπερασμένο σώμα. Ισχύουν τα εξής.*

i) Αν E είναι υπόσωμα του K, τότε $|K| = q^n$, όπου $q = |E|$ και $n = [K : E]$.

ii) $|K| = p^n$, όπου p είναι η χαρακτηριστική του K και $n = [K : \mathbb{Z}_p]$.

iii) Κάθε στοιχείο του K είναι ρίζα του πολυωνύμου $f(x) = x^{p^n} - x$ και το K είναι σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Z}_p$, όπου $n = [K : \mathbb{Z}_p]$.

Απόδειξη Τα πρώτα δύο συμπεράσματα αποδείχθηκαν πριν.

Για το iii), έστω $c \in K - \{0_K\}$. Το $K - \{0_K\}$ είναι ομάδα τάξης $p^n - 1$ ως προς τον πολλαπλασιασμό του σώματος K και επομένως η τάξη του c διαιρεί το $p^n - 1$ σύμφωνα με το Θεώρημα του Lagrange. Άρα $c^{p^n-1} = 1_K$ οπότε $f(c) = 0$.

Αν $K = \{c_1, c_2, ..., c_{p^n}\}$, τότε είναι σαφές ότι $\mathbb{Z}_p(c_1, c_2, ..., c_{p^n}) = K$ και $(x - c_1)(x - c_2)...(x - c_{p^n}) = x^{p^n} - x$.

Το συμπέρασμα iii) της παραπάνω πρότασης λέει ότι αν K είναι πεπερασμένο σώμα με p^n στοιχεία, τότε το πολυώνυμο $x^{p^n} - x$ αναλύεται πλήρως πάνω από το K και κάθε στοιχείο του K είναι ρίζα του.

Για το επόμενο αποτέλεσμα χρειαζόμαστε την εξής παρατήρηση. Αν K είναι σώμα χαρακτηριστικής $p > 0$, τότε $(a + b)^p = a^p + b^p$ για κάθε $a, b \in K$ σύμφωνα με την άσκηση 6.1 Λίγο πιο γενικά έχουμε

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

για κάθε θετικό ακέραιο n. Αφήνουμε την επαγωγική απόδειξη ως άσκηση.

Θεώρημα 9.2 (**ύπαρξη κι μοναδικότητα**)

i) Για κάθε πρώτο αριθμό p και κάθε θετικό ακέραιο n υπάρχει πεπερασμένο σώμα K με $|K| = p^n$.

ii) Δυο πεπερασμένα σώματα είναι ισόμορφα αν και μόνο αν έχουν το αυτό πλήθος στοιχείων.

Απόδειξη i) Θεωρούμε το πολυώνυμο $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Έστω K σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Z}_p$ και $E = \{c \in K \mid f(c) = 0\}$. Θα δείξουμε ότι $E = K$.

Το E είναι υπόσωμα του K. Πράγματι, $0_F, 1_F \in E$. Επίσης, αν $c, d \in E$, τότε

- $c+d \in E$ αφού $(c+d)^{p^n} = c^{p^n} + d^{p^n} = c+d$
- $cd \in E$ αφού $(cd)^{p^n} = c^{p^n} d^{p^n} = cd$.

Επειδή το E είναι πεπερασμένο σύνολο, οι παραπάνω σχέσεις δίνουν ότι το $(E,+)$ είναι υποομάδα της $(K,+)$ και το $(E-\{0_F\},\cdot)$ είναι υποομάδα της $(K-\{0_F\},\cdot)$, όπου $+$ και $\cdot$ είναι η πρόσθεση και ο πολλαπλασιασμός αντίστοιχα του K.

Επειδή το K είναι σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Z}_p$ και το $E = \{c \in K \,|\, f(c) = 0\}$ είναι σώμα, παίρνουμε $E = K$.

Αφού $f'(x) = p^n x^{p^n-1} - 1 = -1$ έχουμε μκδ$(f(x), f'(x)) = 1$. Άρα οι ρίζες του $f(x)$ στο K είναι απλές (Πρόταση 0.6). Άρα $|E| \geq \deg f(x)$. Από την άλλη μεριά ξέρουμε ότι κάθε μη μηδενικό πολυώνυμο $f(x)$ με συντελεστές από σώμα έχει το πολύ $\deg f(x)$ ρίζες σε κάθε επέκταση του σώματος. Άρα $|E| \leq \deg f(x)$. Συνεπώς $|E| = \deg f(x)$ και $|K| = |E| = \deg f(x) = p^n$.

ii) Έστω K_1, K_2 πεπερασμένα σώματα με p^n στοιχεία. Από το i) και την Πρόταση 9.1 έπεται ότι τα K_1, K_2 είναι σώματα ριζών του $x^{p^n} - x \in \mathbb{Z}_p[x]$. Άρα τα K_1, K_2 είναι ισόμορφα σύμφωνα με το Πόρισμα 3.6.

Παράδειγμα Τα πολυώνυμα $g(x) = x^3 + x + 1, h(x) = x^3 + x^2 + 1$ είναι ανάγωγα πάνω από το $\mathbb{Z}_2$ γιατί είναι τρίτου βαθμού και δεν έχουν ρίζα στο $\mathbb{Z}_2$. Άρα οι δακτύλιοι $\mathbb{Z}_2[x]/(g(x))$ και $\mathbb{Z}_2[x]/(h(x))$ είναι σώματα. Τα σώματα αυτά έχουν 2^3 στοιχεία γιατί το καθένα είναι $\mathbb{Z}_2$-διανυσματικός χώρος διάστασης 3 (Θεώρημα 0.4). Άρα είναι ισόμορφα σύμφωνα με το Θεώρημα 9.2.

Υποσώματα

Το θεώρημα 9.2 λέει ότι τα πεπερασμένα σώματα ταξινομούνται ως προς ισομορφισμό από το πλήθος των στοιχείων τους. Θα δούμε τώρα πως ταξινομούνται τα υποσώματα πεπερασμένου σώματος.

Θεώρημα 9.3 (υποσώματα πεπερασμένου σώματος) *Έστω K πεπερασμένο σώμα με p^n στοιχεία.*

i) Αν E είναι υπόσωμα του K, τότε $|E| = p^m$, όπου $m|n$.

ii) Για κάθε θετικό διαιρέτη m του n υπάρχει μοναδικό υπόσωμα του K με p^m στοιχεία.

Απόδειξη i) Αν $|E| = q$, τότε από την Πρόταση 9.1, συμπεραίνουμε ότι $|K| = q^k$, όπου $k = [K:E]$. Επειδή το p είναι πρώτος, από $p^n = q^k$ και τη μοναδικότητα της παραγοντοποίησης στους ακέραιους παίρνουμε $q = p^m$, όπου $mk = n$.

ii) Έστω m θετικός διαιρέτης του n, $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ και $g(x) = x^{p^m} - x \in \mathbb{Z}_p[x]$.

Ύπαρξη: Επειδή το m διαιρεί το n, το $p^m - 1$ διαιρεί το $p^n - 1$ καθώς, αν $n = ms$ τότε

$$p^n - 1 = (p^m - 1)((p^m)^{s-1} + (p^m)^{s-2} + \ldots + p^m + 1).$$

Άρα το πολυώνυμο $x^{p^m-1} - 1$ διαιρεί το $x^{p^n-1} - 1$ γιατί αν $a = bc$, τότε

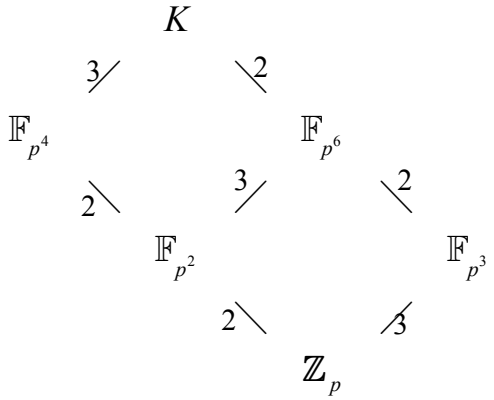
$$x^a - 1 = (x^b - 1)((x^b)^{c-1} + (x^b)^{c-2} + \ldots + x^b + 1).$$

Επομένως το $g(x)$ διαιρεί το $f(x)$. Από την Πρόταση 9.1 ξέρουμε ότι κάθε στοιχείο του K είναι ρίζα του $f(x)$. Έστω $E = \{c \in K \,|\, g(c) = 0\}$. Τότε σύμφωνα με την απόδειξη του Θεωρήματος 9.2 το E είναι σώμα και έχει p^m στοιχεία.

Μοναδικότητα: Αν E_1, E_2 είναι υποσώματα του K με p^m στοιχεία, τότε κάθε στοιχείο του E_1 και κάθε στοιχείο του E_2 είναι ρίζα του $g(x)$ κατά την Πρόταση 9.1. Όμως το $g(x)$ δεν μπορεί να έχει περισσότερες από $\deg g(x) = p^m$ ρίζες στο K. Άρα $E_1 = E_2$.

Στα παρακάτω θα συμβολίζουμε το μοναδικό (ως προς ισομορφισμό) σώμα με p^m στοιχεία με $\mathbb{F}_{p^m}$.

Παράδειγμα 9.4 Έστω K πεπερασμένο σώμα με p^{12} στοιχεία. Από το Θεώρημα 9.3 υπάρχει 1-1 και επί αντιστοιχία μεταξύ των υποσωμάτων του K και των θετικών διαιρετών του 12. Το διάγραμμα των υποσωμάτων του K είναι το ακόλουθο. Έχουμε ταυτίσει το $\mathbb{F}_p$ με το $\mathbb{Z}_p$.



Καλό είναι να συγκριθεί το Θεώρημα 9.3 με το θεώρημα ταξινόμησης υποομάδων πεπερασμένης κυκλικής ομάδας[1] (και το παραπάνω διάγραμμα με το διάγραμμα υποομάδων κυκλικής ομάδας τάξης 12, βλ. Παράδειγμα 9.8 παρακάτω).

Πολλαπλασιαστική ομάδα πεπερασμένου σώματος

Αν K είναι σώμα, τότε το σύνολο $K^* = K - \{0_K\}$ είναι ομάδα με πράξη τον πολλαπλασιασμό του K. Θα λέμε ότι το K^* είναι η **πολλαπλασιαστική ομάδα** του K. Θα δείξουμε στη συνέχεια το σημαντικό αποτέλεσμα ότι η πολλαπλασιαστική ομάδα πεπερασμένου σώματος είναι κυκλική ομάδα. Για το σκοπό αυτό υπενθυμίζουμε τα εξής.

i) *Έστω G πεπερασμένη κυκλική ομάδα τάξης d. Το πλήθος των στοιχείων της G τάξης d είναι η τιμή $\varphi(d)$ της συνάρτησης φ του Euler.*

Πράγματι, αν $G = < g > = \{1, g, g^2, .., g^{d-1}\}$ είναι κυκλική τάξης d, τότε για κάθε k η τάξη του στοιχείου g^k είναι $d/\text{μκδ}(d,k)$. Έχουμε $d/\text{μκδ}(d,k) = d \Leftrightarrow \text{μκδ}(d,k) = 1$.

ii) $n = \sum_{d|n} \varphi(d)$. (Βλ. για παράδειγμα, Παρατήρηση 6.4 i)).

Θεώρημα 9.5 Έστω K πεπερασμένο σώμα. Τότε η πολλαπλασιαστική ομάδα του K είναι κυκλική.

Απόδειξη Έστω d θετικός διαιρέτης του $n = |K^*|$. Αφού το K είναι σώμα, το πολυώνυμο $x^d - 1 \in K[x]$ έχει το πολύ d ρίζες στο K. Άρα

η ομάδα K^* έχει το πολύ μία κυκλική υποομάδα τάξης d. (1)

[1] Βλ. Θεώρημα 4.6.3, *Μια Εισαγωγή στην Άλγεβρα*, Δ. Βάρσος et al, Γ΄Έκδοση, Εκδόσεις Σοφία, 2012.

Θέτουμε $k_d =$ το πλήθος των στοιχείων της K^* τάξης d. Τότε $n = \sum_{d|n} k_d$. Επίσης, από την υπενθύμιση i) και το (1) έπεται ότι $k_d \le \varphi(d)$. Από τις σχέσεις $n = \sum_{d|n} \varphi(d)$ και $n = \sum_{d|n} k_d$ έπεται ότι $k_d = \varphi(d)$. Ειδικά, $k_n = \varphi(n) > 0$. Δηλαδή η ομάδα K^* έχει στοιχείο τάξης n.

Σημείωση Η απόδειξη του προηγούμενου θεωρήματος δείχνει κάτι λίγο πιο γενικό: Έστω K σώμα (όχι αναγκαστικά πεπερασμένο). Τότε κάθε πεπερασμένη υποομάδα της K^* είναι κυκλική.

Παράδειγμα Για κάθε πρώτο αριθμό p η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική σύμφωνα με το προηγούμενο θεώρημα. Για παράδειγμα, αν $p = 11$ τότε οι δυνάμεις του $2 \in \mathbb{Z}_{11}$ είναι

$$2,\ 4,\ 8,\ 16 = 5,\ 10,\ 20 = 9,\ 18 = 7,\ 14 = 3,\ 6,\ 12 = 1.$$

Άρα το $2 \in \mathbb{Z}_{11}$ έχει τάξη 10 και είναι ένας γεννήτορας της $\mathbb{Z}_{11}^*$. Οι δυνάμεις του $5 \in \mathbb{Z}_{11}$ είναι

$$5,\ 25 = 3,\ 15 = 4,\ 20 = 9,\ 45 = 1,$$

οπότε το 5 έχει τάξη 5 στην ομάδα $\mathbb{Z}_{11}^*$. Εύκολα επαληθεύεται ότι οι γεννήτορες της $\mathbb{Z}_{11}^*$ είναι οι 2,6,7,8. Γενικά δεν είναι γνωστός ένας 'απλός τύπος' που δίνει τους γεννήτορες της $\mathbb{Z}_p^*$.

Πόρισμα 9.6 *Έστω επέκταση $E \subseteq K$, όπου το K είναι πεπερασμένο σώμα.*

i) Υπάρχει $a \in K$ με $K = E(a)$.

ii) Η ομάδα Galois $Gal(K,E)$ είναι κυκλική τάξης $n = [K:E]$ και ένας γεννήτορας είναι ο ισομορφισμός $\sigma : K \to K, \sigma(c) = c^q$, όπου $q = |E|$.

Απόδειξη i) Η ομάδα K^* είναι κυκλική. Αν a είναι ένας γεννήτοράς της, τότε $K = E(a)$.

ii) Η απεικόνιση $\sigma : K \to K, \sigma(c) = c^q$, είναι ομομορφισμός σωμάτων. Πράγματι, έχουμε $(c_1 c_2)^q = {c_1}^q {c_2}^q$ για κάθε $c_i \in K$. Ξέρουμε ότι $q = p^m$, όπου p είναι η χαρακτηριστική του K (Πρόταση 9.1). Συνεπώς $(c_1 + c_2)^q = {c_1}^q + {c_2}^q$ για κάθε $c_i \in K$.

Είναι σαφές ότι $Ker\sigma = \{0_K\}$ και άρα ο σ είναι μονομορφισμός. Επειδή το K είναι πεπερασμένο σύνολο, η 1-1 απεικόνιση σ είναι επί. Ισχύει $\sigma(c) = c$ για κάθε $c \in E$ από την Πρόταση 9.1. Άρα $\sigma \in Gal(K,E)$.

Εύκολα επαληθεύεται ότι $\sigma^k(c) = c^{q^k}$ για κάθε $c \in K$ και για κάθε θετικό ακέραιο k. Συνεπώς $\sigma^n(c) = c^{q^n} = c$. Δηλαδή $\sigma^n = 1$. Παρατηρούμε ότι αν m είναι θετικός ακέραιος με $m < n$, τότε $\sigma^m \ne 1$, γιατί αλλιώς κάθε στοιχείο του K θα ήταν ρίζα του πολυωνύμου $x^{q^m} - x$ οπότε $|K| \le q^m < q^n$, άτοπο. Άρα η τάξη του στοιχείου $\sigma \in Gal(K,E)$ είναι n.

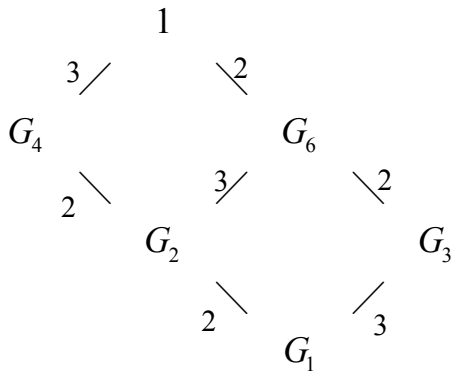
Μέχρι στιγμής έχουμε δείξει ότι η $Gal(K,E)$ περιέχει τουλάχιστον n στοιχεία (τα $1, \sigma, \sigma^2, ..., \sigma^{n-1}$). Έστω τώρα $\tau \in Gal(K,E)$. Έχουμε $K = E(a)$ για κάποιο $a \in K$ σύμφωνα με το i). Ξέρουμε ότι το $\tau(a)$ είναι ρίζα του $Irr(a,E)$ και επίσης ότι $\deg Irr(a,E) = [K:E] = n$. Άρα το $\tau(a)$ μπορεί να πάρει το πολύ n διαφορετικές τιμές, οπότε $|Gal(K,E)| \le n$. Άρα $Gal(K,E) = \{1, \sigma, \sigma^2, ..., \sigma^{n-1}\}$.

Για $E = \mathbb{Z}_p$, ο ισομορφισμός $\sigma : K \to K, \sigma(c) = c^p$ της προηγούμενης πρότασης είναι γνωστός ως ο **αυτομορφισμός του Frobenius.**

Πόρισμα 9.7 Έστω K πεπερασμένο σώμα. Τότε για κάθε θετικό ακέραιο m υπάρχει ανάγωγο $f(x) \in K[x]$ βαθμού m.

Απόδειξη Έστω L σώμα ριζών του $x^{q^m}-x$ πάνω από το K, όπου $q=|K|$. Τότε $[L:K]=m$ και $L=K(a)$ για κάποιο $a\in L$. Το $Irr(a,K)$ έχει βαθμό m.

Παράδειγμα 9.8 Στο διάγραμμα του παραδείγματος 9.4 εφαρμόζουμε την απεικόνιση $Gal(K,-)$. Προκύπτει το ακόλουθο διάγραμμα, όπου $G_m=Gal(K,\mathbb{F}_{p^m})$. Το Πόρισμα 9.6 ii) λέει ότι κάθε G_m είναι κυκλική ομάδα τάξης $12/m$. Συνεπώς έχουμε τους δείκτες υποομάδων που καταγράφονται στις ακμές του διαγράμματος.



Παρατηρούμε ότι λάβαμε το διάγραμμα υποομάδων της κυκλικής ομάδας $G_1=Gal(K,\mathbb{Z}_p)$ που έχει τάξη 12.

Παρατήρηση 9.9 Στο προηγούμενο παράδειγμα δεν εφαρμόσαμε το θεμελιώδες θεώρημα της θεωρίας Galois (άλλωστε το έχουμε αποδείξει μόνο όταν η χαρακτηριστική είναι 0). Όμως, συνδυάζοντας

- το Πόρισμα 9.6,
- το Θεώρημα 9.3 και
- την ταξινόμηση των υποομάδων πεπερασμένων κυκλικών ομάδων,

συνάγουμε ότι *τα συμπεράσματα του θεμελιώδους θεωρήματος της θεωρίας Galois (Θεώρημα 5.3) αληθεύουν και στην περίπτωση που τα σώματα είναι πεπερασμένα.*

Παρατήρηση 9.10 Το Θεώρημα 9.5 μας επιτρέπει να βρίσκουμε γεννήτορες για ενδιάμεσα σώματα πεπερασμένου σώματος. Έστω K πεπερασμένο σώμα με p^n στοιχεία. Ξέρουμε ότι υπάρχει $a\in K$ με $K^*=<a>$. Αν E είναι υπόσωμα του K, ξέρουμε ότι $|E|=p^m$ όπου $m|n$ (και επιπλέον το E είναι το μοναδικό υπόσωμα του K με p^m στοιχεία). Άρα το p^m-1 διαιρεί το p^n-1. Αν $k=\dfrac{p^n-1}{p^m-1}$, τότε από τη ταξινόμηση των υποομάδων πεπερασμένης κυκλικής ομάδας ξέρουμε ότι η υποομάδα $<a^k>$ είναι η μοναδική υποομάδα της K^* τάξης $\dfrac{p^n-1}{k}=p^m-1$. Άρα $E=\mathbb{Z}_p(a^k)$.

Παράδειγμα 9.11 Έστω K ο δακτύλιος $\mathbb{Z}_2[x]/(x^4+x+1)$ και $a\in K$ η εικόνα του x (οπότε $a^4+a+1=0$ στο K).

1. Το K είναι σώμα.

   Είναι σαφές ότι το $f(x)=x^4+x+1\in\mathbb{Z}_2[x]$ δεν έχει ρίζα στο $\mathbb{Z}_2$. Υπάρχει μοναδικό ανάγωγο πολυώνυμο του $\mathbb{Z}_2[x]$ βαθμού 2, το x^2+x+1. Εύκολα επαληθεύεται ότι η Ευκλείδεια διαίρεση του

$f(x)$ με το x^2+x+1 στο $\mathbb{Z}_2[x]$ δίνει μη μηδενικό υπόλοιπο. Άρα το $f(x)$ είναι ανάγωγο, οπότε το K είναι σώμα.

2. Ισχύει $|K|=16$ και μια βάση του K ως $\mathbb{Z}_2$ -διανυσματικός χώρος είναι το σύνολο $\{1,a,a^2,a^3\}$.
   Από το 1 έπεται ότι $Irr(a,\mathbb{Z}_2)=x^4+x+1$. Άρα το σύνολο $\{1,a,a^2,a^3\}$ είναι μια βάση του K (Πρόταση 1.8). Επομένως $|K|=2^4=16$ (Πρόταση 9.1).
3. Το στοιχείο a είναι γεννήτορας της πολλαπλασιαστικής ομάδας του K.
   Χρησιμοποιώντας τη σχέση $a^4+a+1=0$ έχουμε $a^4=a+1, a^5=a^2+a.$ Από τη βάση στο 2 είναι σαφές ότι $a^3\neq 1$ και $a^5=a^2+a\neq 1$. Επειδή η τάξη του a διαιρεί το $|K^*|=16-1=15$, συμπεραίνουμε ότι αυτή είναι ίση με 15.
4. Η ομάδα Galois $Gal(K,\mathbb{Z}_2)$ είναι κυκλική τάξης 4 και παράγεται από τον ισομορφισμό του Frobenius $\sigma: K\to K, \sigma(c)=c^2$.
   Αυτό έπεται άμεσα από το Πόρισμα 9.6 αφού $[K:\mathbb{Z}_2]=4$.
5. Ισχύει $Irr(a,\mathbb{Z}_2)=x^4+x+1=(x+a)(x+a^2)(x+a^4)(x+a^8)$.
   Είδαμε πριν ότι $Irr(a,\mathbb{Z}_2)=x^4+x+1$. Για την δεύτερη ισότητα παρατηρούμε ότι επειδή το a είναι ρίζα του $Irr(a,\mathbb{Z}_2)$ και το πολυώνυμο αυτό έχει συντελεστές στο $\mathbb{Z}_2$, το $h(a)$ είναι ρίζα του $Irr(a,\mathbb{Z}_2)$ για κάθε $h\in Gal(K,\mathbb{Z}_2)$. Αλλά $Gal(K,\mathbb{Z}_2)=\{1,\sigma,\sigma^2,\sigma^3\}$ σύμφωνα με το 4. Άρα τα στοιχεία $a,\sigma(a)=a^2,\sigma^2(a)=a^4,\sigma^3(a)=a^8$ είναι ρίζες του $Irr(a,\mathbb{Z}_2)$. Τα στοιχεία αυτά είναι διακεκριμένα γιατί $K=\mathbb{Z}_2(a)$ και οι ισομορφισμοί $1,\sigma,\sigma^2,\sigma^3$ είναι διακεκριμένοι. Συνεπώς

$$\begin{aligned} Irr(a,\mathbb{Z}_2) &= \prod_{h\in Gal(K,\mathbb{Z}_2)}(x-h(a)) = \\ &= (x-a)(x-a^2)(x-a^4)(x-a^8) = \\ &= (x+a)(x+a^2)(x+a^4)(x+a^8). \end{aligned}$$

6. Για κάθε υπόσωμα E του K θα βρούμε $b\in K$ με $E=\mathbb{Z}_2(b)$.
   Έχουμε $|K|=2^4$ και οι θετικοί διαιρέτες του 4 είναι οι 1,2,4. Από το Θεώρημα 9.3 έπεται ότι το διάγραμμα των υποσωμάτων του K είναι

$$\begin{array}{c} K \\ | \ \} 2 \\ E \\ | \ \} 2 \\ \mathbb{Z}_2 \end{array}$$

   Εφαρμόζοντας της Παρατήρηση 9.10 έχουμε $E=\mathbb{Z}_2(a^k)$, όπου $k=\dfrac{2^4-1}{2^2-1}=5.$
7. Θα βρούμε το $Irr(a^5,\mathbb{Z}_2)$ και το $Irr(a,E)$.
   Όπως αναφέραμε στο 1, υπάρχει μοναδικό ανάγωγο πολυώνυμο στο $\mathbb{Z}_2[x]$ βαθμού 2 πάνω από το $\mathbb{Z}_2[x]$, το x^2+x+1. Επειδή $\deg Irr(a^5,\mathbb{Z}_2)=[\mathbb{Z}_2(a^5):\mathbb{Z}_2]=[E:\mathbb{Z}_2]=2$ όπως είδαμε στο 6, έχουμε $Irr(a^5,\mathbb{Z}_2)=x^2+x+1$.

Για την εύρεση του $Irr(a,E)$ μπορούμε να επιχειρηματολογήσουμε όπως στο 5. Σύμφωνα με το Πόρισμα 9.6 έχουμε $Gal(K,E)=\{1,\sigma\}$, όπου εδώ $\sigma(a)=a^4$. Άρα

$$Irr(a,E)=\prod_{h\in Gal(K,E)}(x-h(a))=(x-a)(x-a^4)=$$
$$=x^2+(a+a^4)x+a^5=x^2+x+a+a^2.$$

8. Αληθεύει ότι το $g(x)=x^4+x^3+1\in\mathbb{Z}_2[x]$ είναι ανάγωγο πάνω από το K;
Δεν αληθεύει.
$1^{ος}$ τρόπος. Όπως στο 1, εύκολα επαληθεύεται ότι το $g(x)$ είναι ανάγωγο πάνω από το $\mathbb{Z}_2$ και επομένως το $L=\frac{\mathbb{Z}_2[x]}{(g(x))}$ είναι σώμα. Επειδή $|L|=2^4=|K|$ υπάρχει ισομορφισμός $h:L\to K$ κατά το Θεώρημα 9.2. Αν $b\in L$ είναι η εικόνα του x, τότε $b^4+b^3+1=0$ στο L. Εφαρμόζοντας την απεικόνιση h, έχουμε $h(b)^4+h(b)^3+1=0$ στο K. Δηλαδή το πολυώνυμο $g(x)$ έχει ρίζα στο K. Επειδή ο βαθμός του είναι μεγαλύτερος του 1, δεν είναι ανάγωγο στο $K[x]$.
$2^{ος}$ τρόπος. Δες το Παράδειγμα 9.14 iii) παρακάτω.

Ανάλυση του $x^{p^n}-x$ πάνω από το $\mathbb{Z}_p$

Ξέρουμε ότι στο $\mathbb{Z}_p[x]$, όπου p πρώτος, ισχύει $x^p-x=x(x-1)(x-2)...(x-(p-1))$. Δηλαδή το x^p-x είναι το γινόμενο όλων των μονικών αναγώγων πολυωνύμων βαθμού 1 πάνω από το $\mathbb{Z}_p$. Πιο γενικά ισχύει το εξής αποτέλεσμα.

Θεώρημα 9.12 *Έστω p πρώτος.*

i) Έστω $g(x)\in\mathbb{Z}_p[x]$ ανάγωγο βαθμού m. Τότε $g(x)\,|\,x^{p^n}-x \Leftrightarrow m\,|\,n$.

ii) Το $x^{p^n}-x$ είναι ίσο με το γινόμενο όλων των μονικών αναγώγων πολυωνύμων στο $\mathbb{Z}_p[x]$ που έχουν βαθμό διαιρέτη του n.

Απόδειξη i) Έστω K σώμα ριζών του $x^{p^n}-x$ πάνω από το $\mathbb{Z}_p$. Αν $g(x)\,|\,x^{p^n}-x$, τότε το K περιέχει ρίζα a του $g(x)$. Τότε $\mathbb{Z}_p(a)\subseteq K$ και $[\mathbb{Z}_p(a):\mathbb{Z}_p]=m$. Συνεπώς $m\,|\,n$ σύμφωνα με το Θεώρημα 9.3.

Αντίστροφα, έστω $m\,|\,n$. Τότε το p^m-1 διαιρεί το p^n-1 και κατά συνέπεια το $x^{p^m}-x$ διαιρεί το $x^{p^n}-x$ (βλ. απόδειξη του θεωρήματος 9.3). Αν a είναι ρίζα του $g(x)$ (σε κάποια επέκταση του $\mathbb{Z}_p$), τότε το $\mathbb{Z}_p(a)$ είναι σώμα με p^m στοιχεία. Άρα κάθε στοιχείο του $\mathbb{Z}_p(a)$ είναι ρίζα του $x^{p^m}-x\in\mathbb{Z}_p[x]$. Επειδή το a είναι ρίζα του $x^{p^m}-x$, το a είναι ρίζα του $g(x)$ και το $g(x)$ είναι ανάγωγο πάνω από το $\mathbb{Z}_p[x]$, παίρνουμε $g(x)\,|\,x^{p^m}-x$.

ii) Επειδή το $\mathbb{Z}_p$ είναι σώμα, ξέρουμε ότι το $x^{p^n}-x$ αναλύεται σε γινόμενο αναγώγων μονικών πολυωνύμων $f_1(x),...,f_t(x)\in\mathbb{Z}_p[x]$ κατά τρόπο ουσιαστικά μοναδικό. Επειδή οι ρίζες του $x^{p^n}-x$ (σε οποιαδήποτε επέκταση του $\mathbb{Z}_p$) είναι απλές, τα $f_i(x)$ είναι διακεκριμένα. Το ζητούμενο έπεται από το i).

Πόρισμα 9.13 Έστω p,q πρώτοι. Τότε το πλήθος των μονικών αναγώγων πολυωνύμων βαθμού q πάνω από το $\mathbb{Z}_p$ είναι ίσο με $\frac{p^q-p}{q}$.

Απόδειξη Σύμφωνα με το προηγούμενο θεώρημα, το $x^{p^q}-x$ είναι ίσο με το γινόμενο α) των μονικών πολυωνύμων βαθμού 1 στο $\mathbb{Z}_p[x]$ και β) των μονικών αναγώγων πολυωνύμων βαθμού q στο $\mathbb{Z}_p[x]$.

Λαμβάνοντας βαθμούς έχουμε $p^q = p+qt$, όπου t το πλήθος των πολυωνύμων στο β). Άρα $t=\dfrac{p^q-p}{q}$.

Παραδείγματα 9.14

i) Το πλήθος των μονικών αναγώγων πολυωνύμων βαθμού 5 πάνω από το $\mathbb{Z}_3$ είναι ίσο με $\dfrac{3^5-3}{5}=48$.

ii) Σύμφωνα με το Θεώρημα 9.12, κάθε μονικό ανάγωγο πολυώνυμο βαθμού 3 πάνω από το $\mathbb{Z}_2$ είναι παράγοντας του $x^{2^3}-x$. Με πράξεις διαπιστώνουμε ότι

$$\begin{aligned} x^{2^3}-x = x^8-x = x(x^7-1) = \\ = x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1) = \\ = x(x-1)(x^3+x^2+1)(x^3+x+1) \end{aligned}$$

και τα τέσσερα πολυώνυμα στο δεξί μέλος είναι ανάγωγα πάνω από το $\mathbb{Z}_2$. Άρα το σύνολο των (μονικών) αναγώγων πολυωνύμων βαθμού 3 πάνω από το $\mathbb{Z}_2$ είναι το $\{x^3+x^2+1,\ x^3+x+1\}$.

iii) Το $g(x)=x^4+x^3+1\in\mathbb{Z}_2[x]$ δεν είναι ανάγωγο πάνω από το σώμα $K=\mathbb{Z}_2[x]/(x^4+x+1)$ (βλ. Παράδειγμα 9.11). Πράγματι, όπως στο Παράδειγμα 9.11 1, το $g(x)$ είναι ανάγωγο πάνω από το $\mathbb{Z}_2$ και από το Θεώρημα 9.12, $g(x)\Big|x^{2^4}-x$. Επειδή το $x^{2^4}-x$ αναλύεται πλήρως πάνω από το K, το ίδιο συμβαίνει με το $g(x)$.

Ασκήσεις 9

1. Ποιο είναι το διάγραμμα υποσωμάτων σώματος που έχει p^{20} στοιχεία, όπου p πρώτος; Ποιο είναι το διάγραμμα υποομάδων κυκλικής ομάδας τάξης 20;
2. Έστω K ο δακτύλιος $\mathbb{Z}_2[x]/(x^4+x^3+1)$ και $a\in K$ η εικόνα του x (οπότε $a^4+a^3+1=0$ στο K).
   a. Δείξτε ότι το K είναι σώμα και βρείτε τα διαγράμματα των υποσωμάτων του K και των υποομάδων της $Gal(K,\mathbb{Z}_2)$.
   b. Αληθεύει ότι το a είναι ένας γεννήτορας της πολλαπλασιαστικής ομάδας του K;
   c. Παραστήστε κάθε ενδιάμεσο σώμα στη μορφή $\mathbb{Z}_2(b)$, όπου b είναι πολυώνυμο του a βαθμού το πολύ 3.
   d. Αληθεύει ότι το x^4+x+1 είναι ανάγωγο πάνω από το K; Ίδιο ερώτημα για το x^4+x^2+1.
   e. Δείξτε ότι αν ένα ενδιάμεσο σώμα περιέχει το a^2, τότε είναι ίσο με το K.
   f. Έστω $\psi: K\to K$ η απεικόνιση που ορίζεται από $\psi(c)=ac$. Δείξτε ότι η ψ είναι $\mathbb{Z}_2$-γραμμική, υπολογίστε τον πίνακά της ως προς τη βάση $1,a,a^2,a^3$ του K και βρείτε το ελάχιστο πολυώνυμο της ψ (με την έννοια της γραμμικής άλγεβρας). Βρήκατε το ίδιο με το $Irr(a,\mathbb{Z}_2)=x^4+x^3+1$;
3. Έστω $f(x)=x^2+2\in\mathbb{Z}_5[x]$ και K σώμα με 125 στοιχεία.
   a. Δείξτε ότι το $f(x)$ είναι ανάγωγο πάνω από το K.
   b. Πόσα στοιχεία έχει τα σώμα $K[x]/(f(x))$ και ποιο είναι το διάγραμμα των υποσωμάτων του;

c. Αληθεύει ότι κάθε ανάγωγο πολυώνυμο βαθμού 25 πάνω από το $\mathbb{Z}_5$ αναλύεται πλήρως πάνω από το $K[x]/(f(x))$;

4. Έστω K πεπερασμένο σώμα τέτοιο ώστε δεν υπάρχει $a \in K$ με $-1 = a^2$. Δείξτε ότι υπάρχει $b \in K$ με $2 = b^2$ ή $-2 = b^2$.
5. Ποιο είναι το πλήθος των σωμάτων που έχουν χαρακτηριστική 2, πλήθος στοιχείων το πολύ 1000 και ακριβώς 3 υποσώματα;
6. Πόσα στοιχεία έχει ένα σώμα ριζών του $(x^2+x+1)(x^3+x+1)$ πάνω από το $\mathbb{Z}_5$;
7. Έστω p,q πρώτοι. Βρείτε το πλήθος των μονικών αναγώγων πολυωνύμων βαθμού q^2 πάνω από το σώμα $\mathbb{Z}_p$;
8. Έστω K πεπερασμένο σώμα με $|K| = p^n$, όπου p πρώτος. Θεωρούμε την απεικόνιση ('ίχνος')

   $Tr : K \to K,\ Tr(a) = a + a^p + a^{p^2} + ... + a^{p^{n-1}}$.

   a. Δείξτε ότι για κάθε $a \in K$, $Tr(a) \in \mathbb{Z}_p$.
   b. Δείξτε ότι η απεικόνιση Tr είναι $\mathbb{Z}_p$-γραμμική.
   c. Αν $b \in K$, ορίζουμε την απεικόνιση $\psi_b : K \to K,\ \psi_b(a) = Tr(ba)$. Δείξτε ότι η ψ_b είναι $\mathbb{Z}_p$-γραμμική απεικόνιση.
   d. Δείξτε ότι $\psi_b = \psi_c \Leftrightarrow b = c$.
   e. Δείξτε ότι κάθε $\mathbb{Z}_p$-γραμμική απεικόνιση $K \to \mathbb{Z}_p$ είναι της μορφής ψ_b, $b \in K$.
9. Έστω p πρώτος, $f(x) = x^p - x + 1 \in \mathbb{Z}_p[x]$ και a μια ρίζα του $f(x)$ σε επέκταση του $\mathbb{Z}_p$. Δείξτε τα εξής.
   a. Το $a+1$ είναι ρίζα του $f(x)$.
   b. Το $\mathbb{Z}_p(a)$ είναι σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Z}_p$.
   c. Το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Z}_p$.
10. Εξετάστε ποιες από τις παρακάτω προτάσεις αληθεύουν. Με K συμβολίζουμε πεπερασμένο σώμα χαρακτηριστικής p.
    a. Υπάρχει πεπερασμένο σώμα με 100 στοιχεία.
    b. Υπάρχει πεπερασμένο σώμα του οποίου η πολλαπλασιαστική ομάδα έχει 100 στοιχεία.
    c. Τα σώματα $\mathbb{Z}_3[x]/(x^2+1)$ και $\mathbb{Z}_3[x]/(x^2+x+2)$ είναι ισόμορφα.
    d. Αν $|K| = q$, τότε $x^q - x = \prod_{a \in K} (x-a)$.
    e. Αν $|K| = p^6$, τότε $\sum_E [K:E] = 12$, όπου το E διατρέχει τα υποσώματα του K.
    f. Η πολλαπλασιαστική ομάδα του $\mathbb{Z}_{61}$ περιέχει στοιχείο τάξης 15.

10. Απαντήσεις - υποδείξεις ασκήσεων

Ασκήσεις 0

1.
   a. Ανάγωγο.
   b. Ανάγωγο.
   c. Ανάγωγο. Δοκιμάστε αναγωγή modulo 2.
   d. Όχι ανάγωγο (το 1 είναι ρίζα).
   e. Ανάγωγο. Δοκιμάστε αναγωγή modulo 2 σε κατάλληλο αριθμητικό πολλαπλάσιο του πολυωνύμου.
   f. Ανάγωγο. (Κριτήριο του Eisenstein για $p = 3$.)
2. Αν, για παράδειγμα, $a = 2^n \cdot 5$ τότε εφαρμόζει το κριτήριο του Eisenstein για $p = 5$.
3.
   a. Εφαρμόστε την τεχνική του Παραδείγματος 0.5 iii), δηλαδή θεωρήστε το $(x+1)^8 + 1$.
   b. Εφαρμόστε το κριτήριο του Eisenstein στο πολυώνυμο $p!(1 + x + \frac{x^2}{2!} + ... + \frac{x^p}{p!})$.
4.
5. Όλες είναι σωστές.

Ασκήσεις 1

1.
2. Από $[K:L][L:F] = [K:F] =$ πρώτος, έπεται ότι $[K:L] = 1$ ή $[L:F] = 1$, δηλαδή $L = K$ ή $L = F$.
3.
   a. $Irr(\sqrt{1+\sqrt{7}}, \mathbb{Q}) = x^4 - 2x^2 - 6$. Πράγματι, έστω $a = \sqrt{1+\sqrt{7}}$. Τότε $a^2 = 1 + \sqrt{7}$ και $(a^2 - 1)^2 = 7 \Rightarrow a^4 - 2a^2 - 6 = 0$. Δηλαδή το a είναι ρίζα του πολυωνύμου $x^4 - 2x^2 - 6$. Από το κριτήριο του Eisenstein για $p = 2$ έπεται ότι το πολυώνυμο αυτό είναι ανάγωγο πάνω από το $\mathbb{Q}$. Επειδή είναι μονικό έχουμε $Irr(a, \mathbb{Q}) = x^4 - 2x^2 - 6$.
   b. $Irr(\sqrt{1+\sqrt{7}}, \mathbb{Q}(\sqrt{7})) = x^2 - 1 - \sqrt{7}$. Πράγματι, είδαμε πριν ότι το a ικανοποιεί τη σχέση $a^2 = 1 + \sqrt{7}$, δηλαδή είναι ρίζα του πολυωνύμπυ $x^2 - 1 - \sqrt{7} \in \mathbb{Q}(\sqrt{7})[x]$. Άρα $\deg Irr(a, \mathbb{Q}(\sqrt{7})) = 1$ ή 2. Αν ισχύει η πρώτη περίπτωση, τότε $a \in \mathbb{Q}(\sqrt{7})$ και επομένως $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{7}) \Rightarrow [\mathbb{Q}(a):\mathbb{Q}] \le [\mathbb{Q}(\sqrt{7}):\mathbb{Q}] = 2$, πράγμα άτοπο αφού από το προηγούμενο ερώτημα έχουμε $[\mathbb{Q}(a):\mathbb{Q}] = \deg Irr(a, \mathbb{Q}) = 4$. Άρα $\deg Irr(a, \mathbb{Q}(\sqrt{7})) = 2$ και επομένως $Irr(a, \mathbb{Q}(\sqrt{7})) = x^2 - 1 - \sqrt{7}$.
   c. $Irr(\sqrt{2} + i, \mathbb{R}) = x^2 - 2\sqrt{2}x + 3$.
   d. $Irr(\sqrt{2} + i, \mathbb{Q}) = x^4 - 2x^2 + 9$.
4. b. Οι ρίζες του $Irr(a, \mathbb{Q}) = x^2 + x - 1$ είναι $(-1 \pm \sqrt{5})/2$ και επομένως $a = (-1 \pm \sqrt{5})/2$. Από αυτό έπεται ότι $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{5})$. Από $\pm\sqrt{5} = 2a + 1$ έπεται ότι $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(a)$ και άρα έχουμε ισότητα.

Έχουμε $a=\zeta_5+\zeta_5^{-1}=\cos(2\pi/5)+i\sin(2\pi/5)+\cos(2\pi/5)-i\sin(-2\pi/5)=2\cos(2\pi/5)$. Επειδή η γωνία $2\pi/5$ είναι στο πρώτο τεταρτημόριο, έχουμε $\cos(2\pi/5)\geq 0$ και άρα $a\geq 0$, οπότε $a=(-1+\sqrt{5})/2$. Άρα $\cos(2\pi/5)=(-1+\sqrt{5})/4$.

5. $Irr(a,\mathbb{Q})=x^4-2p^2x+p^2-p$ και $Irr(a,\mathbb{Q}(\sqrt{p}))=x^2-p-\sqrt{p}$.

6.

a. Όχι. Από Eisenstein το x^5+3x^2+6x+3 είναι ανάγωγο πάνω από το $\mathbb{Q}$ και άρα $[\mathbb{Q}(a):\mathbb{Q}]=5$ για κάθε ρίζα a του x^5+3x^2+6x+3. Αν κάποια ρίζα a ανήκει στο K, τότε $9=[K:\mathbb{Q}]=[K:\mathbb{Q}(a)][\mathbb{Q}(a):\mathbb{Q}]$, δηλαδή το 5 διαιρεί το 9, αδύνατο.

b. Από την υπόθεση έπεται ότι κάθε διαδοχική επέκταση στην αλυσίδα

$$\mathbb{Q}\subseteq\mathbb{Q}(a_1)\subseteq\mathbb{Q}(a_1,a_2)\subseteq\ldots\subseteq\mathbb{Q}(a_1,a_2,\ldots,a_{n-1})\subseteq\mathbb{Q}(a_1,a_2,\ldots,a_n)$$

έχει βαθμό 1 ή 2. Άρα

$$[\mathbb{Q}(a_1,\ldots,a_n):\mathbb{Q}]=[\mathbb{Q}(a_1):\mathbb{Q}][\mathbb{Q}(a_1,a_2):\mathbb{Q}(a_1)]\ldots[\mathbb{Q}(a_1,\ldots,a_n):\mathbb{Q}(a_1,\ldots,a_{n-1})]$$

είναι δύναμη του 2.

7. Έχουμε τις διαδοχικές επεκτάσεις $F\subseteq F(a^2)\subseteq F(a)$, όπου $[F(a):F]$ περιττός. Επειδή $[F(a):F]=[F(a):F(a^2)][F(a^2):F]$, έπεται ότι $[F(a):F(a^2)]$ περιττός. Αλλά το a είναι ρίζα του $x^2-a^2\in F(a^2)[x]$. Άρα $[F(a):F(a^2)]=\deg Irr(a,F(a^2))\leq 2$. Συνεπώς $\deg Irr(a,F(a^2))=1$ που σημαίνει ότι $a\in F(a^2)$, δηλαδή $F(a)\subseteq F(a^2)$. Συνεπώς $F(a)=F(a^2)$.

8.

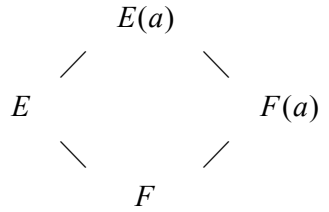
a. Από τις διαδοχικές επεκτάσεις $F\subseteq F(a)\subseteq F(a,b)$ και το Θεώρημα 1.7 έπεται ότι $m\big|[F(a,b):F]$. Όμοια $n\big|[F(a,b):F]$ και επειδή $\mu\kappa\delta(m,n)=1$ έχουμε $mn\big|[F(a,b):F]$. Δείξτε ότι $[F(a,b):F]\leq mn$.

b. $\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2})=\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{2})\Rightarrow[\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{2}):\mathbb{Q}]=12$ από το a.

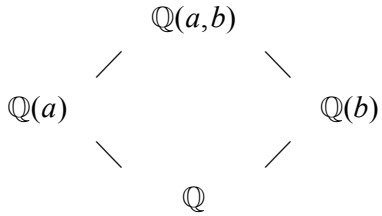
9.

a. Από τορισμό του $Irr(a,E)$ έχουμε $\deg Irr(a,E)\leq\deg Irr(a,F)$ και το ζητούμενο έπεται από την Πρόταση 1.5 ii).

b. Θεωρήστε τις παρακάτω επεκτάσεις και χρησιμοποιήστε το a.



10. Θεωρήστε το διάγραμμα



11. Το $a-2$ είναι ρίζα του $(x+2)^3-(x+2)^2+(x+2)+1=x^3+5x^2+9x+7$ και άρα $\frac{1}{a-2}=-\frac{1}{7}((a-2)^2+5(a-2)+9)$. Απάντηση: $\frac{a^2}{a-2}=a+2+\frac{4}{a-2}=\frac{1}{7}(2+3a-4a^2)$.

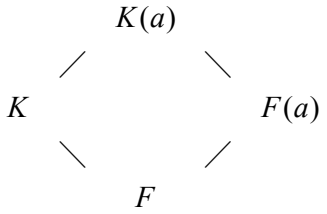
12.

a. Δεν υπάρχει καθώς τα i και $\sqrt{2}$ δεν είναι συζυγή πάνω από το $\mathbb{Q}$.

b. Υπάρχει.

c. Υπάρχει.

13. Επειδή $F \subseteq K$ υπάρχει ρίζα a του $f(x)$ σε επέκταση του K. Έχουμε $Irr(a,K)\big|Irr(a,F)$.



Άρα $[K(a):K] \le [F(a):F]$. Από το διάγραμμα έπεται ότι $[F(a):F]\big|[K(a):K][K:F]$ που από την υπόθεση δίνει $[F(a):F]\big|[K(a):K]$. Άρα $[K(a):K] = [F(a):F]$, δηλ. $\deg Irr(a,K) = \deg Irr(a,F)$. Από αυτό έπεται και $Irr(a,K)\big|Irr(a,F)$ έπεται ότι $Irr(a,K) = Irr(a,F)$. Άρα το $Irr(a,F)$ είναι ανάγωγο πάνω από το K.

14. Οι συνεπαγωγές $a \Rightarrow b$ και $b \Rightarrow c$ αποδειχτηκαν στην απόδειξη της Πρότασης 1.5 και η συνεπαγωγή $c \Rightarrow a$ στην Παρατήρηση μετά τα Παραδείγματα 1.6.
15.
16.
    a. Σ.
    b. Λ. Αν $\zeta_5 \in \mathbb{Q}(\zeta_7)$, τότε από το Θεώρημα 1.7, $[\mathbb{Q}(\zeta_5):\mathbb{Q}]\big|[\mathbb{Q}(\zeta_7):\mathbb{Q}]$. Από το Παράδειγμα 1.6 iii) έπεται ότι $4\big|6$, άτοπο.
    c. Σ.
    d. Σ. Ανήκουν στη βάση $\{1,a,...,a^7\}$ του $\mathbb{Q}(a)$, όπου $a = \sqrt[8]{2}$.
    e. Σ.
    f. Λ. Στο Παράδειγμα 1.8 ii) είδαμε ότι $[\mathbb{Q}(\rho,\omega):\mathbb{Q}] = 6$. Επειδή το $\rho\omega$ είναι ρίζα του $x^3 - 5 \in \mathbb{Q}[x]$, έχουμε $[\mathbb{Q}(\rho\omega):\mathbb{Q}] \le 3$. Άρα $[\mathbb{Q}(\rho\omega):\mathbb{Q}] \ne [\mathbb{Q}(\rho,\omega):\mathbb{Q}] \Rightarrow \mathbb{Q}(\rho,\omega) \ne \mathbb{Q}(\rho\omega)$.
    g. Σ.

Ασκήσεις 2

1.
2. Δεν είναι πεπερασμένη αφού για κάθε n, $[F:\mathbb{Q}] \ge [\mathbb{Q}(\sqrt[2^n]{3}):\mathbb{Q}] = 2^n$ καθώς $Irr(\sqrt[2^n]{3},\mathbb{Q}) = x^{2^n} - 3$.
3. Αν η επέκταση $F \subseteq K$ είναι πεπερασμένη, υπάρχει πεπερασμένη βάση $\{a_1,...,a_n\}$ του K ως διανυσματικός χώρος πάνω από το F.
4. Η επέκταση $\mathbb{Q}(a+b,ab) \subseteq \mathbb{Q}(a,b)$ είναι αλγεβρική καθώς τα a,b είναι ρίζες του πολυωνύμου $x^2 - (a+b)x + ab \in \mathbb{Q}(a+b,ab)$. Θεωρήστε τις διαδοχικές επεκτάσεις $\mathbb{Q} \subseteq \mathbb{Q}(a+b,ab) \subseteq \mathbb{Q}(a,b)$ και το Πόρισμα 2.4.
5. Έστω $[F:\mathbb{Q}] < \infty$ και $a \in F$. Τότε $a \in \mathbb{Q}(\pi)$ και το a είναι αλγεβρικό πάνω από το $\mathbb{Q}$ σύμφωνα με το Θεώρημα 2.2. Άρα $a = \dfrac{f(\pi)}{g(\pi)}$, όπου $f(x), g(x) \in \mathbb{Q}[x]$ και $\mu\kappa\delta(f(x),g(x)) = 1$, και το a είναι ρίζα πολυωνύμου $a_n x^n + ... + a_1 x + a_0 \in \mathbb{Q}[x]$ θετικού βαθμού. Αντικαθιστώντας και απαλοίφοντας τους παρονομαστές παίρνουμε $a_n f(\pi)^n + a_{n-1} f(\pi)^{n-1} g(\pi) + ... + a_1 f(\pi) g(\pi)^{n-1} + a_0 g(\pi)^n = 0$. Επειδή το π δεν είναι αλγεβρικό πάνω από το $\mathbb{Q}$ έχουμε

$$a_n f(x)^n + a_{n-1} f(x)^{n-1} g(x) + ... + a_1 f(x) g(x)^{n-1} + a_0 g(x)^n = 0.$$

Από αυτό και $\mu\kappa\delta(f(x),g(x))=1$ έπεται ότι $g(x)\big|f(x)$. Αν $f(x)=h(x)g(x),$ παίρνουμε $a_n h(x)^n+\ldots+a_1h(x)+a_0=0.$ Θεωρώντας μεγιστοβάθμιους όρους στην τελευταία σχέση συμπεράινουμε ότι το $h(x)$ είναι σταθερό πολυώνυμο, $h(x)=c\in\mathbb{Q}.$ Άρα $\dfrac{f(\pi)}{g(\pi)}=h(\pi)=c\in\mathbb{Q}.$

6.
7. Αν ήταν κατασκευάσιμο με κανόνα και διαβήτη, τότε η γωνία 40^o θα ήταν κατασκευάσιμη και άρα η γωνία 20^o θα ήταν κατασκευάσιμη, πράγμα αδύνατο όπως είδαμε.
8. Χρησιμοποιήστε ότι το $\cos(\theta/3)$ είναι ρίζα του $4x^3-3x-\cos\theta$. [Σημείωση. Για τη μια κατεύθυνση θα πρέπει να αποδειχθεί ότι οι πραγματικές ρίζες τριωνύμου κατασκευάζονται από τους συντελεστές του.]
9. Από την Ευκλείδεια Γεωμετρία ξέρουμε ότι το κανονικό κυρτό πεντάγωνο και το κανονικό κυρτό εξάγωνο κατασκευάζονται, δηλ. οι γωνίες 72^o και 60^o κατασκευάζονται. Άρα η γωνία $72^o-60^o=12^o$ κατασκευάζεται και διχοτομώντας δύο φορές, η γωνία 3^o κατασκευάζεται. Από την άλλη μεριά, ούτε η γωνία 1^o ούτε η γωνία 2^o κατασκευάζεται γιατί αλλιώς θα κατασκευαζόταν η γωνία 20^o, πράγμα αδύνατο.
10.
    a. Σ.
    b. Σ.
    c. Λ. Ένα αντιπαράδειγα είναι $a=b=$μη αλγεβρικό στοιχείο.
    d. Σ.

Ασκήσεις 3

1.
    a. Είναι.
    b. Είναι.
    c. Δεν είναι.
    d. Είναι.
2.
    a. 2.
    b. 4.
    c. 2.
    d. 6.
    e. 3.
3. $K=\mathbb{Q}(\sqrt{3},\sqrt{5})$. Από την απόδειξη του Θεωρήματος 3.7 έπεται ότι μια επιλογή είναι $a=\sqrt{3}+\sqrt{5}$.
4.
5. Αν $\rho\in K-F$, δείξτε ότι $K=F(\rho)$. Το $Irr(\rho,F)$ είναι της μορφής $Irr(\rho,F)=x^2+ax+b$. Τότε η άλλη ρίζα του $Irr(\rho,F)$ είναι η $-a-\rho$ και επομένως $K=F(\rho)=F(\rho,-a-\rho)$ που είναι σώμα ριζών.
6.
    a. Έπεται από τον ορισμό σώματος ριζών.
    b. $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{Q}(\sqrt[3]{2},i)$.
    c. $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt[4]{2})$.
7.
    a. Από την άσκηση 2.3 υπάρχουν $a_i\in K$ με $K=F(a_1,\ldots,a_n)$. Θεωρήστε το γινόμενο $Irr(a_1,F)\ldots Irr(a_n,F)$.

b. Έστω K, L σώματα ριζών πάνω από το F και $f(x) \in F[x]$ ανάγωγο με ρίζα στο $K \cap L$. Επειδή το K είναι σώμα ριζών πάνω από το F, από το Θεώρημα 3.9 το $f(x)$ αναλύεται πλήρως πάνω από το K. Ομοίως, το $f(x)$ αναλύεται πλήρως πάνω από το L. Από τη μοναδικότητα της παραγοντοποίησης πολυωνύμων σε γινόμενο ανάγωγων οι δυο παραγοντοποιήσεις ταυτίζονται οπότε το $f(x)$ αναλύεται πληρως πάνω από το $K \cap L$. Από το προηγούμενο ερώτημα έπεται ότι το $K \cap L$ είναι σώμα ριζών πάνω από το F.

8. Από το Θεώρημα 3.7 έχουμε $K = F(a)$ για κάποιο a. Αν $b \in \mathbb{C}$ είναι ρίζα του $Irr(a, \mathbb{Q})$, τότε από το Πόρισμα 1.10 υπάρχει μονομορφισμός $K \to \mathbb{C}$ που στέλνει το a στο b. Άρα $b \in K$. Συνεπώς το K είναι σώμα ριζών του $Irr(a, \mathbb{Q})$.
9. Από το μικρό θεώρημα του Fermat έπεται ότι $x^p - x = x(x-1)(x-2)...(x-(p-1))$ στο $\mathbb{Z}_p[x]$.
10.
11. Οι ρίζες του $f(x)$ στο $\mathbb{Z}_3(a)$ είναι οι $a, a^3 = a-1, a^9 = a+1$.
12.
    a. Δείξτε ότι αν το a είναι ρίζα του $f(x)$ στο K, τότε το $a+1$ είναι επίσης ρίζα.
    b. Δείξτε ότι όλοι οι ανάγωγοι παράγοντες του $f(x)$ πάνω από το F έχουν τον ίδιο βαθμό.
13.
    a. Δείξτε ότι το a είναι ρίζα του $p(x) = x^4 - 2x^2 - 6$. Από το κριτήριο του Eisentein το $p(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$. Το $p(x)$ έχει μη πραγματική ρίζα καθώς $p(x) = (x^2 - (1+\sqrt{7}))(x^2 - (1-\sqrt{7}))$ και $1 - \sqrt{7} < 0$. Από το Θεώρημα 3.9 έπεται ότι αν το $\mathbb{Q}(a)$ ήταν σώμα ριζών πάνω από το $\mathbb{Q}$, τότε όλες οι ρίζες του $p(x)$ θα ήταν στο $\mathbb{Q}(a)$. Αυτό είναι άτοπο καθώς $\mathbb{Q}(a) \subseteq \mathbb{R}$.
    b. Δείξτε ότι το b είναι ρίζα του $q(x) = x^4 - 8x^2 + 9$ και ότι $q(x) = (x-b)(x+b)(x-c)(x+c)$ στο $\mathbb{C}[x]$, όπου $c = \sqrt{4 - \sqrt{7}}$. Επειδή $bc = \sqrt{4^2 - (\sqrt{7})^2} = 3 \in \mathbb{Q}$ και $b \in \mathbb{Q}(b)$ παίρνουμε $c \in \mathbb{Q}(b)$. Άρα το $\mathbb{Q}(b)$ είναι σώμα ριζών του $q(x)$ πάνω από το $\mathbb{Q}$.
14. Ξέρουμε ότι $[K : F] \le n!$, όπου $\deg f(x) = n$ (Θεώρημα 3.4 και Πόρισμα 3.6). Αν $a \in K$ είναι ρίζα του $p(x)$, τότε $F(a) \subseteq K$ και $[K : F] = [K : F(a)][F(a) : F] = [K : F(a)]p$ οπότε $p \mid [K : F]$. Αυτό είναι άτοπο καθώς κάθε θετικός ακέραιος μικρότερος ή ίσος του $n!$ δεν έχει πρώτο διαρέτη p με $p > n$.
15. Έστω $\sqrt[3]{2} \in K$. Από το Θεώρημα 3.9 έπεται ότι κάθε ρίζα του $Irr(\sqrt[3]{2}, \mathbb{Q})$ ανήκει στο K. Δείξτε ότι $i\sqrt{3} \in K$. Από την υπόθεση της μοναδικότητας έπεται ότι $i\sqrt{3} \in \mathbb{Q}(i\sqrt{2})$. Δείξτε ότι αυτό είναι άτοπο.
16.
17.
    a. Κάθε στοιχείο του F είναι της μορφής $\frac{f(\pi)}{g(\pi)}$, όπου $f(x), g(x) \in \mathbb{Q}[x]$. Χρησιμοποιώντας ότι το π δεν είναι αλγεβρικό πάνω από το $\mathbb{Q}$, δείξτε με πράξεις ότι το $p(x)$ δεν έχει ρίζα στο F. Άρα $3 \mid [K : F]$. Δείξτε ότι το $p(x)$ έχει μη πραγματική ρίζα και επομένως $2 \mid [K : F]$. Το ζητούμενο έπεται από την ανισότητα στο Θεώρημα 3.4 (που ισχύει για κάθε σώμα ριζών από το Πόρισμα 3.6).
    b. Εφαρμόστε το Λήμμα 3.5 για $F_1 = \mathbb{Q}(\pi)$ και $F_2 = \mathbb{Q}(e)$
18.
    a. Σ.
    b. Λ.
    c. Σ.
    d. Λ.
    e. Σ.

f. Λ.

Ασκήσεις 4

1.
   a. $\mathbb{Z}_2 \times \mathbb{Z}_2$.
   b. $\mathbb{Z}_2$.
   c. $\mathbb{Z}_2$.
   d. $\mathbb{Z}_2$.
   e. $\mathbb{Z}_2$.
2. $\mathbb{Z}_2$ (το πολυώνυμο δεν είναι ανάγωγο).
3. Δείξτε ότι η απεικόνιση $K \to K, a \mapsto \overline{a}$, όπου ο $\overline{a}$ είναι ο μιγαδικός συζυγής του a, είναι στοιχείο της $Gal(K, \mathbb{Q})$ και έχει τάξη 2.
4. S_3.
5. $Irr(\sqrt{2}-2\sqrt{3}, \mathbb{Q}) = (x-(\sqrt{2}-2\sqrt{3}))(x-(\sqrt{2}+2\sqrt{3})(x-(-\sqrt{2}-2\sqrt{3})(x-(-\sqrt{2}+2\sqrt{3}) =$
   $= x^4 - 28x^2 + 100.$
6.
7.
   a. Για να δείξουμε ότι η ομάδα Galois, που έχει τάξη 4 σύμφωνα με το Παράδειγμα 4.9 ii), είναι κυκλική, αρκεί να βρούμε ένα στοιχείο της σ τέτοιο ώστε $\sigma^2 \neq 1$. Για το σκοπό αυτό δείξτε ότι υπάρχει $\sigma \in Gal(\mathbb{Q}(\sqrt{2+\sqrt{2}}), \mathbb{Q})$ με $\sigma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}$ και δείξτε για αυτό το σ ότι $\sigma^2 \neq 1$.
   b. Δείξτε ότι το $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ είναι σώμα ριζών πάνω από το $\mathbb{Q}$. Από αυτό έπεται ότι η ομάδα Galois έχει τάξη 4. Αν σ είναι στοιχείο της ομάδας Galois τότε $\sigma(\sqrt{2+\sqrt{3}}) \in \{\sqrt{2+\sqrt{3}}, -\sqrt{2+\sqrt{3}}, \sqrt{2-\sqrt{3}}, -\sqrt{2-\sqrt{3}}\}$. Σε κάθε περίπτωση δείξτε ότι $\sigma^2 = 1$. (Βλ. και Παράδειγμα 4.9 iii)).
8. Επειδή $\deg f(x) = 3$, αν το $f(x)$ δεν ήταν ανάγωγο πάνω από το $\mathbb{Q}$, τότε η ομάδα Galois $Gal(K, \mathbb{Q})$ θα είχε το πολύ $2!$ στοιχεία, άτοπο.
9. $b \Rightarrow c$: Δείξτε ότι αν $|Gal(K:\mathbb{Q})| = 3$ και a ρίζα του $p(x)$, τότε $K = \mathbb{Q}(a)$.
10.
   a. Δείξτε ότι αν $\sigma \in Gal(\mathbb{R}, \mathbb{Q})$ και $a < b$, τότε $\sigma(a) < \sigma(b)$. Στη συνέχεια χρησιμοποιήστε την πυκνότητα των ρητών στο $\mathbb{R}$.
   b. Δείξτε ότι για κάθε $a \in \mathbb{Q}$, υπάρχει $\sigma_a \in Gal(\mathbb{Q}(\pi), \mathbb{Q})$ με $\sigma_a(\pi) = \pi + a$.
11.
12.
   a. $[K:\mathbb{Q}] = 4$.
   b. $Irr(a, \mathbb{Q}) = x^4 - 3x^2 + 4$, $Irr(a, \mathbb{Q}(a^2)) = x^2 - \frac{3+i\sqrt{7}}{2}$, $Irr(a^2, \mathbb{Q}) = x^2 - 3x + 4$.
   c. Ναι.
   d.
   e. Όχι.
13.
14. Θεωρήστε τις διαδοχικές επεκτάσεις $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[4]{p}\right) \subseteq \mathbb{Q}\left(\sqrt[4]{p}, i\right)$ για να συμπεράνετε ότι $[\mathbb{Q}\left(\sqrt[4]{p}, i\right) : \mathbb{Q}] = 8$ και εφαρμόστε το Θεώρημα 4.6
15.

a. Χρησιμοποιώντας την Πρόταση 4.10 δείξτε ότι αν $f(x) = f_1(x)f_2(x)$, τότε η G είναι ισόμορφη με υποομάδα της $S_{n_1} \times S_{n_2}$ όπου $n_i = \deg f_i(x)$. Αν $n_i \geq 1$, τότε $n_1!n_2! < (n_1+n_2)!$, άτοπο.

b. Δείξτε ότι αν $Gal(\mathbb{Q}(a), \mathbb{Q}) \neq 1$, τότε το $\mathbb{Q}(a)$ περιέχει τουλάχιστον 2 ρίζες του $f(x)$ και επομένως $|Gal(K, \mathbb{Q}(a))| \leq (n-2)!$ από την Πρόταση 4.10. Τότε έχουμε $[K:\mathbb{Q}] = [K:\mathbb{Q}(a)][\mathbb{Q}(a):\mathbb{Q}] \leq (n-2)!n < n!$, άτοπο.

16.

a. Λ.

b. Λ. Ένα αντιπαράδειγμα είναι $F = K_1 = \mathbb{Q}$ και $K_2 = \mathbb{Q}(\sqrt[3]{2})$ (Βλ. Παράδειγμα 4.3 i))

c. Λ. Πρόταση 4.10 (το 16 δεν διαιρεί το 4!).

Ασκήσεις 5

1. $a = (1+i)\rho$.
2. Έπεται από το διάγραμμα υποσωμάτων του Παραδείγματος 5.7.
3. Επειδή η S_3 έχει μοναδική υποομάδα δείκτη 2, από το θεμελιώδες θεώρημα έπεται ότι το K έχει μοναδικό υπόσωμα βαθμού 2 άνω από το $\mathbb{Q}$. Συνεπώς αν είχαμε $\sqrt{5} \in K$ και $\sqrt{7} \in K$, τότε $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{7})$. Δείξτε ότι αυτό είναι αδύνατο.
4. Έπεται από το διάγραμμα υποσωμάτων του Παραδείγματος 5.7.
5.
   a. Χρησιμοποιήστε το θεμελιώδες θεώρημα και το γεγονός ότι για κάθε διαιρέτη d της τάξης πεπερασμένης κυκλικής ομάδας υπάρχει ακριβώς μία υποομάδα τάξης d.
   b.
   c.
   d. Χρησιμοποιήστε το Θεώρημα 3.9.
   e.
6. Χρησιμοποιώντας αναλύσεις σε γινόμενα ξένων κύκλων, δείξτε ότι ομάδα S_4 έχει 9 στοιχεία τάξης 2 και εφαρμόστε το θεμελιώδες θεώρημα.
7. Παρατηρήστε ότι το a είναι ρίζα του $x^2 - (a+a^{-1})x + 1 \in \mathbb{Q}(a+a^{-1})$.
8. Χρησιμοποιώντας το θεμελιώδες θεώρημα, δείξτε ότι αν $i \in K$, τότε το πλήρες διάγραμμα των υποσωμάτων του K είναι της μορφής

$$\begin{array}{c} K = \mathbb{Q}(i,a) \\ | \\ \mathbb{Q}(i) \\ | \\ \mathbb{Q} \end{array}$$

   Ποιο από τα τρία σώματα είναι το $\mathbb{Q}(a)$;
9.
   a. $Irr(\zeta_7, \mathbb{Q}) = x^6 + x^5 + .. + x + 1$ (Παράδειγμα 1.7 iv)) και επειδή το K είναι σώμα ριζών του $Irr(\zeta_7, \mathbb{Q})$, έχουμε $|G| = [K:\mathbb{Q}] = 6$ (Θεώρημα 4.6).
   b.
   c.
   d. Δείξτε ότι $\zeta_7^3 + \zeta_7^5 + \zeta_7^6 \notin \mathbb{R}$.
10.

a. Το $p(x)$ αναλύεται πλήρως στο $K[x]$ από το Θεώρημα 3.9. Έστω $p(x)=(x-a_1)...(x-a_n)$, $a_i \in K$. Ξέρουμε ότι για κάθε $\sigma \in G$ το $\sigma(a)$ είναι ένα από τα $a_1,...,a_n$. Έστω $i \in \{1,..,n\}$. Στο γινόμενο $\prod_{\sigma\in G}(x-\sigma(a))$ θα μετρήσουμε το πλήθος των σ που ικανοποιούν $\sigma(a)=a_i$.

Από το από το Πόρισμα 3.11 υπάρχει $\tau \in G$ με $\tau(a)=a_i$. Τώρα

$$\sigma(a)=a_i=\tau(a) \Leftrightarrow \tau^{-1}\sigma(a)=a \Leftrightarrow \tau^{-1}\sigma \in Gal(K,F(a)) \Leftrightarrow \sigma=\tau h,\ h \in Gal(K,F(a)).$$

Άρα πλήθος των σ που ικανοποιούν $\sigma(a)=a_i$ είναι ίσο με $|Gal(K,F(a))|=[K:F(a)]$, όπου η τελευταία ισότητα έπεται από το Θεώρημα 4.6. Συνεπώς

$$\prod_{\sigma\in G}(x-\sigma(a))=(x-a_1)^m..(x-a_n)^m=((x-a_1)..(x-a_n))^m=p(x)^m,$$

όπου $m=[K:F(a)]$.

b. Εφαρμόζοντας το a. και την άσκηση 9b προκύπτει (πράξεις) ότι $Irr(\zeta_7+\zeta_7^{\,6},\mathbb{Q})=x^3+x^2-2x-1$.

11. c. Η $Gal(K,\mathbb{Q})$ δεν είναι κυκλική.
12. Υπάρχει $a \in K$ με $K=F(a)$. Εφαρμόστε το θεμελιώδες θεώρημα στην επέκταση $F \subseteq L$ όπου L σώμα ριζών του $Irr(a,F)$ πάνω από το F.
13.
    a. Θεώρημα 5.8.
    b.
    c. Όχι, γιατί το μοναδικό υπόσωμα του K βαθμού 2 πάνω από το $\mathbb{Q}$ είναι το $\mathbb{Q}(i\sqrt{31})$ και $\mathbb{Q}(i\sqrt{31}) \neq \mathbb{Q}(i\sqrt{3})$.
    d. Όχι, γιατί διαφορετικά θα περιείχε όλες τις ρίζες του x^3-x+1 σύμφωνα με το Θεώρημα 3.9. Τότε θα περιείχε το $i\sqrt{23}$ (τετραγωνική ρίζα της διακρίνουσας του x^3-x+1). Όπως στο προηγούμενο υποερώτημα, αυτό είναι άτοπο.
14.
15. Από την υπόθεση ότι η $Gal(K,\mathbb{Q})$ είναι αβελιανή και το Θεώρημα 5.3 iii) έπεται ότι για κάθε σώμα E με $\mathbb{Q} \subseteq E \subseteq K$, το E είναι σώμα ριζών πάνω από το $\mathbb{Q}$.

    Το x^5-2 είναι ανάγωγο πάνω από το $\mathbb{Q}$ σύμφωνα με το κριτήριο του Eisenstein. Αν το K περιέχει ρίζα του x^5-2, τότε το x^5-2 θα αναλύεται πλήρως πάνω από το K (Θεώρημα 3.9), οπότε το K θα περιέχει σώμα ριζών του x^5-2 πάνω από το $\mathbb{Q}$. Ειδικά, το K θα περιείχε το $E=\mathbb{Q}(\sqrt[5]{2})$. Όμως το E δεν είναι σώμα ριζών πάνω από το $\mathbb{Q}$, άτοπο σύμφωνα με αυτό που αναφέραμε πριν.

    Στη συνέχεια, αν $x^5-2=p(x)q(x)$ είναι η παραγοντοποίση σε γινόμενο μονικών αναγώγων με $p(x),q(x) \in K[x]$, $\deg p(x)=2$, $\deg q(x)=3$, δείξτε ότι $\sigma(p(x))=p(x)$ και $\sigma(q(x))=q(x)$ για κάθε $\sigma \in Gal(K,\mathbb{Q})$. Άρα $p(x),q(x) \in \mathbb{Q}[x]$ σύμφωνα με το Θεώρημα 5.3 i). Αυτό είναι άτοπο γιατί το x^5-2 είναι ανάγωγο πάνω από το $\mathbb{Q}$.Αν το x^5-2 έχει ρίζα στο K, τότε το x^5-2 θα αναλύεται πλήρως πάνω από το K (Θεώρημα 3.9), οπότε το K θα περιέχει σώμα ριζών E του x^5-2 πάνω από το $\mathbb{Q}$. Τότε από την υπόθεση ότι η $Gal(K,\mathbb{Q})$ είναι αβελιανή και το Θεώρημα 5.3 iii) έπεται ότι η $Gal(E,\mathbb{Q})$ είναι αβελιανή ως πηλίκο της $Gal(K,\mathbb{Q})$. Δείξτε ότι αυτό είναι άτοπο.
16. Έστω $a \in K$ ρίζα του $f(x)$ και $E=\mathbb{Q}(a) \subseteq K$. Επειδή η ομάδα $G=Gal(K,\mathbb{Q})$ είναι αβελιανή, κάθε υποομάδα της είναι κανονική. Από το Θεώρημα 5.3iii) έπεται ότι το E είναι σώμα ριζών πάνω από το $\mathbb{Q}$. Τώρα αν $b \in K$ είναι ρίζα του $f(x)$, από το Πόρισμα 3.11 έπεται ότι υπάρχει $\sigma \in G$ με $\sigma(a)=b$. Αλλά $\sigma(a) \in E$ σύμφωνα με το Λήμμα 3.8. Δηλαδή $b \in E$. Επειδή η τελευταία σχέση ισχύει για κάθε ρίζα του $f(x)$ και το K είναι σώμα ριζών του $f(x)$, παίρνουμε $K \subseteq E$. Άρα $K=E$. Συνεπώς $|G|=[K:\mathbb{Q}]=[E:\mathbb{Q}]=\deg f(x)=n$.
17.

a. Επειδή το K περιέχει ρίζα του $f(x)$ που είναι ανάγωγο πάνω από το $\mathbb{Q}$ με $\deg f(x) = p$, έχουμε $p \mid [K:\mathbb{Q}]$. Ξέρουμε ότι $[K:\mathbb{Q}] \le p!$ γιατί το K είναι σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$. Συνεπώς $[K:\mathbb{Q}] = pm$, όπου $m \le (p-1)!$. Επειδή p πρώτος έχουμε μκδ$(p,m) = 1$.

b. (Για τη λύση που ακολουθεί χρησιμοιποούμε δράσεις ομάδων). Έστω $G = Gal(K,\mathbb{Q})$. Ξέρουμε ότι η G δρα στο σύνολο των ριζών $\{a_1,...,a_p\}$ του $f(x)$ με $(\sigma, a_i) \mapsto \sigma(a_i)$. (Τα a_i είναι διακεκριμένα αφού $f(x)$ ανάγωγο πάνω από το $\mathbb{Q}$ που έχει χαρακτηριστική 0).

Έστω ότι υπάρχει κανονική υποομάδα $H \le G$ με $|H| = m$. Θεωρούμε τη φυσική δράση της H στο σύνολο $\{a_1,...,a_p\}$. Έχουμε τις τροχιές $O_i = \{h(a_i) \mid h \in H\}$, τις σταθεροποιούσες ομάδες $Stab_i = \{h \in H \mid h(a_i) = a_i\}$ και ξέρουμε από τις δράσεις ομάδων ότι $|O_i| = [H : Stab_i]$.

Ισχυρισμός: Για κάθε i, j έχουμε $|O_i| = |O_j|$.

Απόδειξη: Από την Πρόταση 3.11, ξέρουμε ότι για κάθε a_i, a_j υπάρχει $\sigma \in G$ με $\sigma(a_i) = a_j$. Επειδη η H είναι κανονική στη G έχουμε την απεικόνιση $Stab_i \to Stab_j, h \mapsto \sigma h \sigma^{-1}$, και εύκολα επαληθεύετα ότι είναι $1-1$ και επί. Άρα $|O_i| = |O_j|$.

Επειδή τα σύνολα O_i είναι ισοπληθικά, τα διακεκριμένα από αυτά αποτελούν διαμέριση του $\{a_1,...,a_p\}$ και p είναι πρώτος, συμπεραίνουμε ότι

- για κάθε i, $|O_i| = 1$ ή
- για κάθε i, $O_i = \{a_1,...,a_p\}$.

Στην πρώτη περπτωση έχουμε $H = \{1\}$ που είναι το ζητούμενο. Στη δεύτερη περίπτωση, από τη σχέση $|O_i| = [H : Stab_i]$ έπεται ότι $p \| H|$ που είναι άτοπο λόγω του μκδ$(p,m) = 1$ από το πρώτο ερώτημα.

18.

a. Σ.
b. Σ.
c. Λ. Ένα αντιπαράδειγμα είναι $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) = E = K$.
d. Λ. Ένα αντιπαράδειγμα είναι $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$.

Ασκήσεις 6

1. Επειδή $ab = ba$, ισχύει το διωνυμικό ανάπτυγμα $(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i$. Για κάθε $i = 1,..., p-1$ ο ακέραιος $\binom{p}{i}$ είναι πολλαπλάσιο του p (γιατί;). Από την υπόθεση έπεται ότι $\binom{p}{i} a^{p-i} b^i = 0$, $i = 1,..., p-1$, και επομένως $(a+b)^p = a^p + b^p$.

Με επαγωγή στο n προκύπτει εύκολα ότι $(a_0 + a_1 + ... + a_n)^p = {a_0}^p + {a_1}^p + ... + {a_n}^p$ για κάθε $a_i \in R$. Τώρα για $R = \mathbb{Z}_p[x]$ έχουμε

$$(g(x))^p = (a_n x_n + \ldots + a_1 x + a_0)^p =$$
$$= (a_n x_n)^p + \ldots + (a_1 x)^p + a_0{}^p =$$
$$= a_n{}^p x_n{}^p + \ldots + a_1{}^p x^p + a_0{}^p.$$

Από το μικρό θεώρημα του Fermat, $a_i{}^p = a_i$ (αφού $a_i \in \mathbb{Z}_p$) και επομένως

$$(g(x))^p = a_n x_n{}^p + \ldots + a_1 x^p + a_0 = g(x^p).$$

2. $Irr(\zeta, \mathbb{Q}(\alpha)) = x^2 - \alpha x + 1$, $Gal(\mathbb{Q}(\zeta), \mathbb{Q}(\alpha)) \simeq \mathbb{Z}_2$ (ο γεννήτορας στέλνει το ζ στο ζ^{-1}), $[\mathbb{Q}(a) : \mathbb{Q}] = \varphi(n)/2$.
3. $\Phi_{12}(x) = x^4 - x^2 + 1$ και το $\Phi_{25}(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$.
4.

   a. $x^{p^2} - 1 = (x-1)\Phi_p(x)\Phi_{p^2}(x) \Rightarrow \Phi_{p^2}(x) = \dfrac{(x^p)^p - 1}{x^p - 1} = \Phi_p(x^p).$

   b. Χρησιμοποιώντας τη σχέση
   $$x^{2n} - 1 = \prod_{d|2n} \Phi_d(x) = \prod_{d|n} \Phi_d(x) \prod_{d|n} \Phi_{2d}(x)$$
   δείξτε ότι $x^n + 1 = \prod_{d|n} \Phi_{2d}(x)$ και εφαρμόστε επαγωγή στον περιττό n.

5.

   a. Από την υπόθεση έπεται ότι υπάρχει ισομορφισμός δακτυλίων $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ και επομένως υπάρχει ισομορφισμός ομάδων
   $$U(\mathbb{Z}_{mn}) \simeq U(\mathbb{Z}_m) \times U(\mathbb{Z}_n).$$
   Το ζητούμενο έπεται από την Πρόταση 6.6.

   b. Επειδή $\zeta_m = \zeta_{mn}{}^n, \zeta_n = \zeta_{mn}{}^m$ έχουμε $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$. Από την υπόθεση υπάρχουν $a, b \in \mathbb{Z}$ με $1 = ma + nb$, οπότε
   $$\zeta_{mn} = \zeta_{mn}{}^1 = (\zeta_{mn}{}^m)^a (\zeta_{mn}{}^n)^b = \zeta_n{}^a \zeta_m{}^b \in \mathbb{Q}(\zeta_m, \zeta_n).$$
   Άρα $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m, \zeta_n)$.

   c. Έστω
   $$G = Gal(\mathbb{Q}(\zeta_{mn}), \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)),$$
   $$H_m = Gal(\mathbb{Q}(\zeta_{mn}), \mathbb{Q}(\zeta_m)) \text{ και}$$
   $$H_n = Gal(\mathbb{Q}(\zeta_{mn}), \mathbb{Q}(\zeta_n)).$$
   Έχουμε $H_m, H_n \leq G$ και η G είναι αβελιανή (Πρόταση 6.6). Άρα $H_m H_n \leq G$. Δείξτε τα εξής
   - $|H_m| = \varphi(n)$ και $|H_n| = \varphi(m)$
   - $H_m \cap H_n = \{1\}$.

   Από τα παραπάνω έπεται ότι
   $$|H_m H_n| = \varphi(n)\varphi(m) = \varphi(nm) = |Gal(\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}|$$
   (η τελευταια ισότητα είναι από την Πρόταση 6.6). Επομένως $G = Gal(\mathbb{Q}(\zeta_{mn}), \mathbb{Q})$. Άρα $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ από την αντιστοιχία Galois.

   d. Δείξτε ότι $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_e)$ και $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$, $e = \varepsilon\kappa\pi(m,n)$, $d = \mu\kappa\delta(m,n)$.

6.

   a. Η G_8 έχει τάξη $\varphi(8) = 4$ και δεν είναι κυκλική. Εδώ $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$ και η αναλυτική αντιστοιχία Galois περιέχεται στο Παράδειγμα 5.7.

b. Η G_{10} είναι κυκλική τάξης $\varphi(10)=4$ και ένας γεννήτορας είναι ο ισομορφισμός $\sigma:\mathbb{Q}(\zeta_{10})\to\mathbb{Q}(\zeta_{10})$ που στέλνει το ζ_{10} στο $\zeta_{10}^{\,3}$. Η αντιστοιχία Galois είναι

$$\begin{array}{cc} \mathbb{Q}(\zeta_{10}) & 1 \\ | \ \}2 & | \ \}2 \\ \mathbb{Q}(\zeta_{10}+\zeta_{10}^{-1}) & <\sigma^2> \\ | \ \}2 & | \ \}2 \\ \mathbb{Q} & G=<\sigma> \end{array}$$

7.

a. Με το συμβολισμό του παραδείγματος 6.8, υπολογίστε τα $h(a)$, $h\in<\sigma^2>$. Για παράδειγμα, $\sigma^2(a)=\zeta^4+\zeta^{-4}=2\cos(8\pi/11)$. Ξέρουμε ότι το $h(a)$ είναι ρίζα του $Irr(a,\mathbb{Q})$. Συμπεράνετε ότι $\prod_{h\in<\sigma^2>}(x-h(a))=Irr(a,\mathbb{Q})$. (Βλ. και Πόρισμα 4.5).

b. Δείξτε ότι

- $a\in FixH$, όπου $H=<\sigma^5>\le Gal(\mathbb{Q}(\zeta),\mathbb{Q})=<\sigma>$, και
- $[\mathbb{Q}(a):\mathbb{Q}]>1$.

Από την πρώτη σχέση και την αντιστοιχία Galois έπεται ότι

$$[\mathbb{Q}(a):\mathbb{Q}]\le[FixH:\mathbb{Q}]=[G:H]=2.$$

Από τη δεύτερη σχέση πάιρνουμε $[\mathbb{Q}(a):\mathbb{Q}]=2$.

8.

a. Με άμεσο υπολογισμό ή χρήση της άσκησης 4 βρίσκουμε $\Phi_{14}(x)=x^6-x^5+x^4-x^3+x^2-x+1$.

b. Έστω $a=\zeta_7+\zeta_7^{-1}$. Δρίξτε ότι $Irr(a,\mathbb{Q})=x^3+x^2-2x-1$ με τη μέθοδο του Παραδείγματος 6.8. Στη συνέχεια υπολογίστε τις ρίζες του $Irr(a,\mathbb{Q})$ υπολογίζοντας τις εικόνες του a κάτω από τα στοιχεία της ομάδας Galois $Gal(\mathbb{Q}(\zeta_7),\mathbb{Q})$ (βλ. την άσκηση 5.10 αν σας προβληματίζει η επανάληψη των ριζών). Οι ρίζες είναι

$$2\cos(2\pi/7),\ 2\cos(8\pi/7),\ 2\cos(10\pi/7)$$

(βλ. Παράδειγμα 6.9). Συγκρίνατε συντελεστες του x^2 στην ισότητα $Irr(a,\mathbb{Q})=(x-2\cos(2\pi/7))(x-2\cos(8\pi/7))(x-2\cos(10\pi/7))$ για να λάβετε το ζητούμενο.

c. Αληθεύει.

9. Έστω $\sqrt[3]{2}\in\mathbb{Q}(\zeta_n)$ για κάποιο n. Επειδή το $\mathbb{Q}(\zeta_n)$ είναι σώμα ριζών, από το Θεώρημα 3.9 παίρνουμε ότι το $Irr(\sqrt[3]{2},\mathbb{Q})$ αναλύεται πλήρως στο $\mathbb{Q}(\zeta_n)$ και άρα το $\mathbb{Q}(\zeta_n)$ περιέχει το σώμα $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$. Η ομάδα Galois του $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ πάνω από το $\mathbb{Q}$ δεν είναι αβελιανή (αυτό έπεται με τρόπο παρόμοιο με αυτόν του παραδείγματος 4.3 iii). Όμως αν E είναι υπόσωμα του $\mathbb{Q}(\zeta_n)$, τότε η ομαδα Galois του E πάνω από το $\mathbb{Q}$ είναι αβελιανή (γιατί;). Αυτό είναι άτοπο.

10. Δείξτε ότι $Irr(a,\mathbb{Q})=(x-\zeta-\zeta^2-\zeta^4)(x-\zeta^3-\zeta^5-\zeta^6)=x^2+x+2$ και παρατηρήστε ότι η διακρίνουσα του τριωνύμου είναι -7.

11. $Irr(a,\mathbb{Q})=x^4-x^3-4x^2+4x+1$.

12. Δεν αληθεύει. Ένα αντιπαράδειγμα είναι όταν το a είναι πραγματική ρίζα του x^4+x-1. Τότε $[\mathbb{Q}(a):\mathbb{Q}]=4$ και δεν υπάρχει σώμα E με $\mathbb{Q}\subseteq E\subseteq\mathbb{Q}(a)$ και $[E:\mathbb{Q}]=2$ (γιατί; Το x^4+x-1 έχει ακριβώς 2 πραγματικές ρίζες).

13. b. Θεωρήστε υπόσωμα του $\mathbb{Q}(\zeta_p)$ βαθμού d πάνω από το $\mathbb{Q}$ και εφαρμόστε την αντιστοιχία Galois. (Εδώ θεωρούμε γνωστό ότι η ομάδα Galois του $\mathbb{Q}(\zeta_p)$ είναι κυκλική, βλ. παρατήρηση πριν το Παράδειγμα 6.7).

14.

15. a. Παρόμοιο με το Παράδειγμα 6.8.
    b. Έστω p πρώτος. Αν υπάρχει πρώτος q με $p|q-1$, τότε θεωρώντας την επέκταση $\mathbb{Q}(\zeta_q)$, υπάρχει υπόσωμα βαθμού p πάνω από το $\mathbb{Q}$. (Εδώ θεωρούμε γνωστό ότι η ομάδα Galois του $\mathbb{Q}(\zeta_p)$ είναι κυκλική, βλ. παρατήρηση πριν το Παράδειγμα 6.7). Το ζητούμενο προκύπτει από το Θεώρημα πρωαρχικού στοιχείου.

    Τώρα η ύπαρξη πρώτου q με $p|q-1$ έπεται από το Θεώρημα του Dirichlet για πρώτους σε αριθμητική πρόοδο, πχ βλ. http://mathworld.wolfram.com/DirichletsTheorem.html.
16. Το πλήθος των n με $\varphi(n) \le [K:\mathbb{Q}]$ είναι πεπερασμένο.
17. Είναι τα $n < 300$ τέτοια ώστε το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη.
18.
    a. Σ.
    b. Σ.
    c. Λ. Ένα αντιπαράδειγμα είναι $E = \mathbb{Q}(\sqrt[3]{2})$
    d. Λ. Η ομάδα $Gal(\mathbb{Q}(\zeta_n), E)$ είναι αβελιανή.
    e. Σ.

Ασκήσεις 7

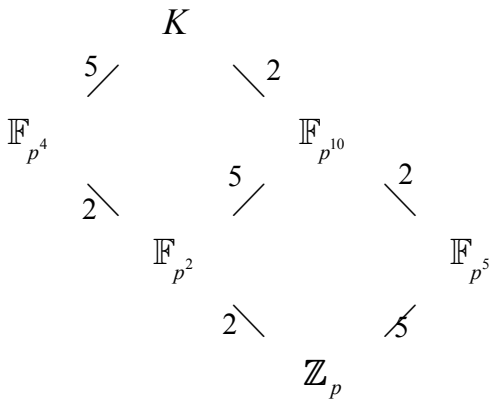
1. Εφαρμόστε το Θεώρημα 5.3 iii) και την Πρόταση 7.5 i).
2.
3. Η ομάδα Galois ανάγωγου πολυωνύμου πάνω από το $\mathbb{Q}$ βαθμού 2, 3 ή 4 είναι ισόμορφη με υποομάδα της S_2, S_3, S_4 και οι ομάδες αυτές είναι επιλύσιμες σύμφωνα με το Παράδειγμα 7.3.
4.
    a. Σ.
    b. Λ. Αλλιώς θα ήταν επιλύσιμη η S_5, πράγμα που δεν αληθεύει, βλ. Θεώρημα 7.5.
    c. Σ.
5. Θεωρήστε την υποομάδα $\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in k\}$.

Ασκήσεις 8

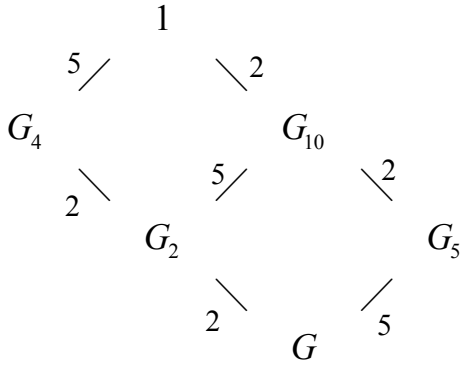
1. Ένα παράδειγμα είναι $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3-\sqrt{2}})$.
2. Βρείτε το σώμα ριζών του πολυωνύμου και δείξτε με τον ορισμό ότι το πολυώνυμο είναι επιλύσιμο με ριζικά. Το ζητούμενο έπεται από το Θεώρημα 8.2.
3. Βλ. Παράδειγμα 8.5.
4. Αληθεύει. Παρατηρήστε ότι το πολυώνυμο παραγοντοποιείται πάνω από το $\mathbb{Q}$.
5. a. Δείξτε ότι το πολυώνυμο είναι επιλύσιμο με ριζικά και άρα η ομάδα Galois είναι επιλύσιμη.
6.
7.
8. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.
    a. Σ.
    b. Λ.
    c. Σ.
    d. Σ.

Ασκήσεις 9

1. Το διάγραμμα υποσωμάτων σώματος που έχει p^{20} στοιχεία, όπου p πρώτος, είναι το ακόλουθο.



Το διάγραμμα υποομάδων κυκλικής πμάδας τάξης p^{20}, όπου p πρώτος, είναι το ακόλουθο. Με G_m συμβολίζουμε κυκλική ομάδα τάξης $12/m$



2. Για τα ερωτήματα a-d βλ. Παράδειγμα 9.11.

   Παρατηρήστε ότι $x^4+x^2+1=(x^2+x+1)^2$.

   Η τάξη του a^2 στην πολλαπλασιαστική ομάδα είναι $\dfrac{2^4-1}{\text{μκδ}(2^4-1,2)}=2^4-1$. Άρα $\langle a^2\rangle=\langle a\rangle$.

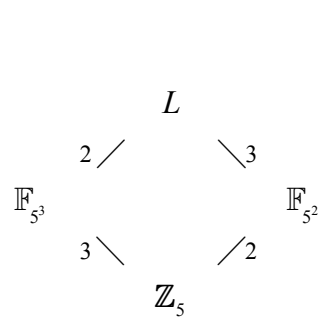
   Ο ζητούμενος πίνακας είναι ο

$$\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}\in M_4(\mathbb{Z}_2)$$

   και το ελάχιστο πολυώνυμό του είναι το x^4+x^3+1.

3. Αν το $f(x)$ δεν ήταν ανάγωγο πάνω από το K, τότε θα είχε ρίζα a στο K γιατί $\deg f(x)=2$. Αλλά τότε $[\mathbb{Z}_5(a):\mathbb{Z}_5]=2$ και το 2 θα διαιρούσαι το $[K:\mathbb{Z}_5]=3$.

   Το σώμα $L=K[x]/(f(x))$ έχει 5^6 στοιχεία. Επειδή οι θετικοί διαιρέτες του 6 είναι οι $1,2,3,6$ το ζητούμενο διάγραμμα είναι το ακόλουθο.



Για το c χρησιμοποιήστε το Θεώρημα 9.12 που λέει ότι κάθε ανάγωγο πολυώνυμο πάνω από το $\mathbb{Z}_5$ βαθμού 5^2 διαιρεί το $x^{5^6} - x$. Στο L το $x^{5^6} - x$ αναλύεται πλήρως.

4. Αρκεί να δειχθεί ότι αν $a \in K$, τότε υπάρχει $b \in K$ με $b^4 = a^2$. Δείξτε ότι η απεικόνιση $\{c^2 \,|\, c \in K\} \to \{c^4 \,|\, c \in K\}$, $c^2 \mapsto c^4$, είναι 1-1 και επί.
5. Δύο. Το ένα έχει 2^4 στοιχεία και το άλλο 2^9 στοιχεία.
6. 5^6.
7. $\dfrac{p^{q^2} - p^q}{q^2}$. Χρησιμοποιήστε τη μέθοδο της απόδειξης του πορίσματος 9.13.
8.
9.
10.
    a. Λ.
    b. Σ.
    c. Σ.
    d. Σ.
    e. Σ.
    f. Σ.